OWASP Portland Chapter

Welcome to OWASP Portland's monthly chapter meeting!

Twitter: @PortlandOWASP

Website: pdxowasp.org

Meetup: https://www.meetup.com/OWASP-Portland-Chapter/

Slack: owasp.slack.com #chapter-pdx

April Chapter Meeting

OWASP Top Ten For Javascript Developers

Presented by: Lewis Ardern

Wednesday April 10, 2019 from 6–8pm

Hosted by: New Relic 111 SW 5th Suite 2700, Portland

https://www.meetup.com/OWASP-Portland-Chapter/events/259395373/

BREACHING THE CYBER SECURITY JOB INDUSTRY

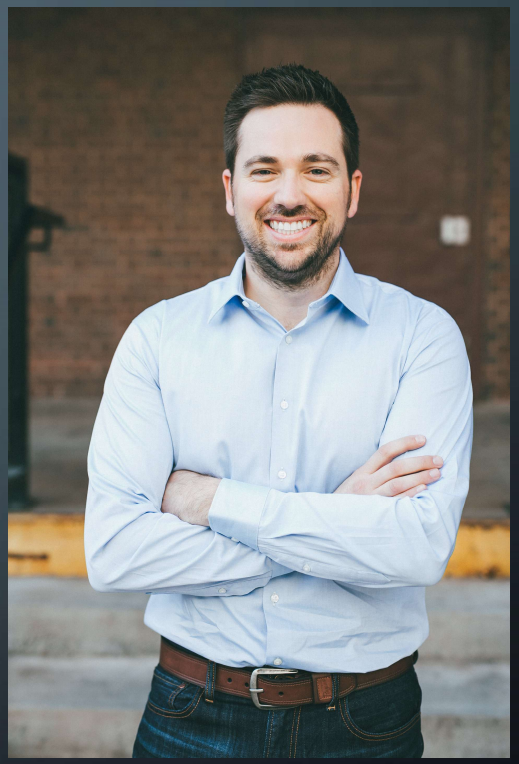
RYAN KRAUSE

PORTLAND, OREGON OWASP CHAPTER MEETING

MARCH 2019

WHO AM I?

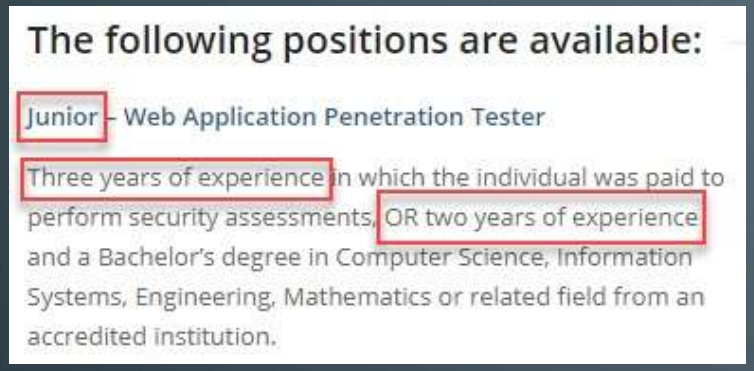
- 11 years in the InfoSec field doing various things
- Currently:
  - Sr. Security Consultant at NetSPI
  - Web application and network penetration testing
- Previously:
  - Security Engineering/AppSec at HP
  - Vulnerability Scanner Development & IT at BeyondTrust
  - Web Development at Comcast
  - Web Development & QA at Western Digital
- Education
  - Computer Engineering, B.S. - UC Irvine (zot zot!)

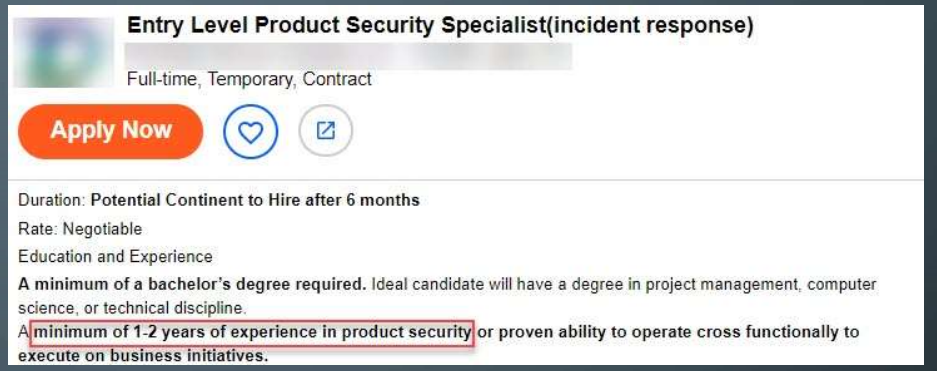


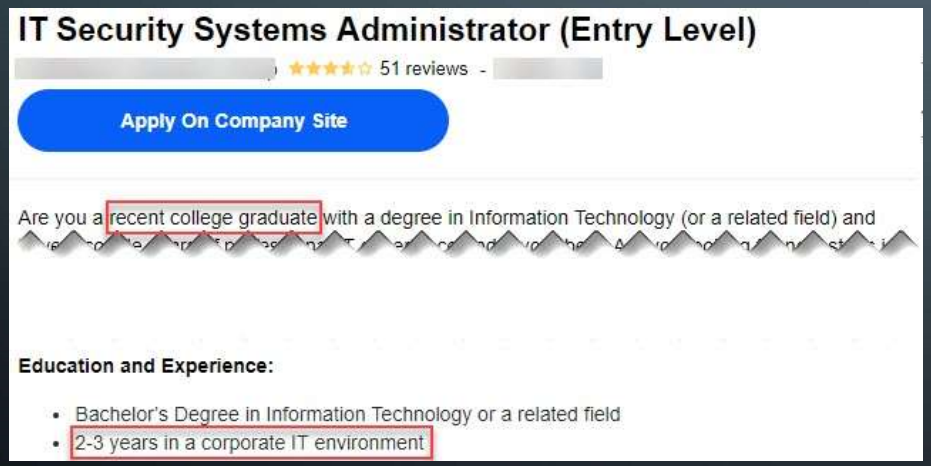
AGENDA

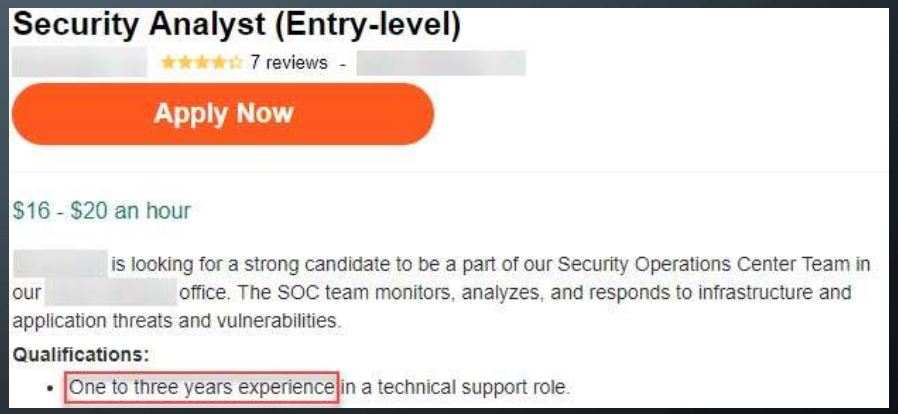
- Why are we here?
- What are some of the challenges job hunters and employers face?
- How can inexperienced candidates get into InfoSec?
- How do you position yourself for success?
- What types of resources are available?

GETTING INTO INFOSEC ISN'T ALWAYS EASY…







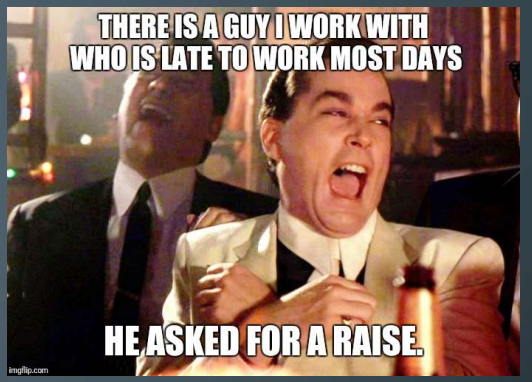



ENTRY LEVEL?!

CHALLENGES - JOB SEEKERS

- Lack of experience
- Too many experienced candidates
- School/training didn't teach what was needed
- Employers want the skillset of three separate job roles
- Employers aren't clear about what they want

CHALLENGES - EMPLOYERS



- Lack of qualified candidates
- Unrealistic candidate expectations
- Low (0%) InfoSec unemployment rate
- Company limitations (salary cap, weak benefits package)
- Poor environment/boring work

THERE IS A GAP…

- "Why are organizations having a hard time hiring?" asks Gary Hayslip, CISO at Webroot […]. He answers, saying, " Organizations at times are trying to hire a unicorn — i.e. they need three people but can only hire one so they write the job spec with a huge list of disparate skill sets that most security professionals don't have."
- "I also believe there's a number of people coming out of school with cyber degrees and they can't get jobs because of minimal experience. Whether they like it or not they need to take those entry level positions and mature as a security professional.

https://cybersecurityventures.com/cybersecurity-unemployment-rate/

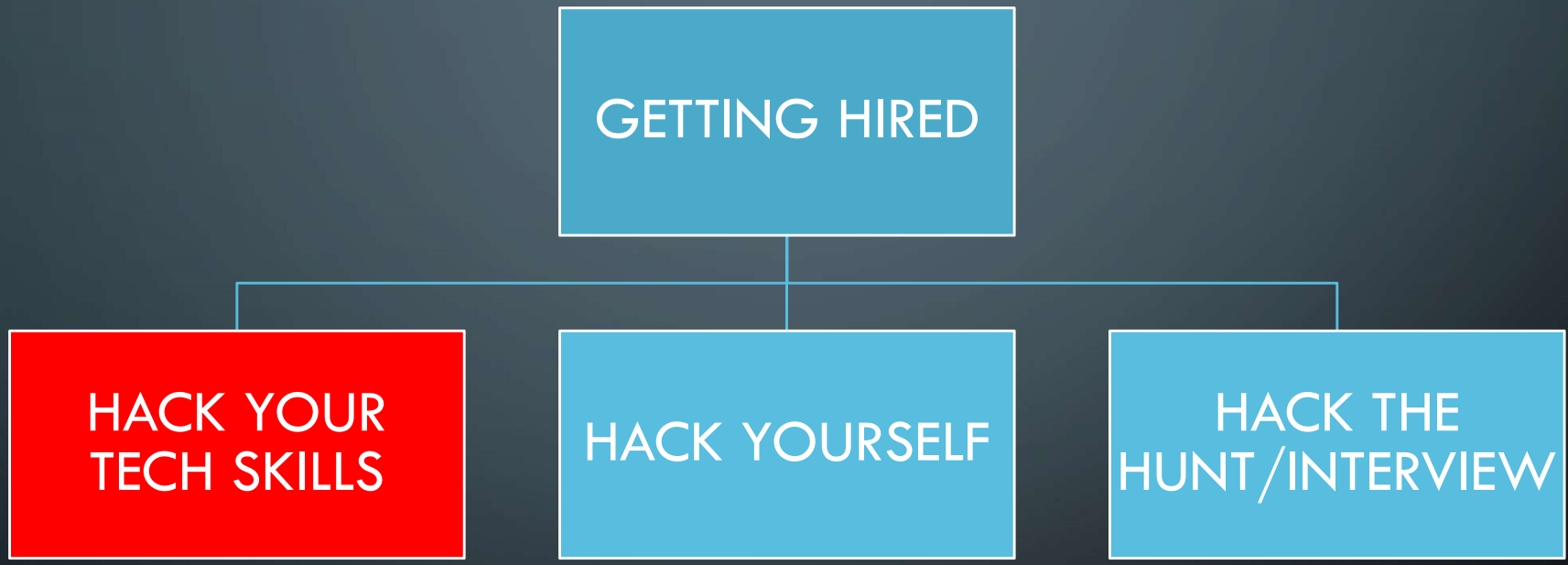
EMPLOYERS ARE REALIZING IT TOO…

- "Organizations are waking up to the critical importance of security," says Jennifer Steffens, CEO at IOActive […] The bad news is the workforce shortage will grow unless organizations also wake up how they approach finding and retaining talent."
- "There is a wealth of talent around the world that wants to engage in this global fight," add Steffens. "They may not be classically trained, have a certain degree, or fit into any mold you've seen before. To succeed we must challenge the norms and embrace a culture that celebrates this diversity."

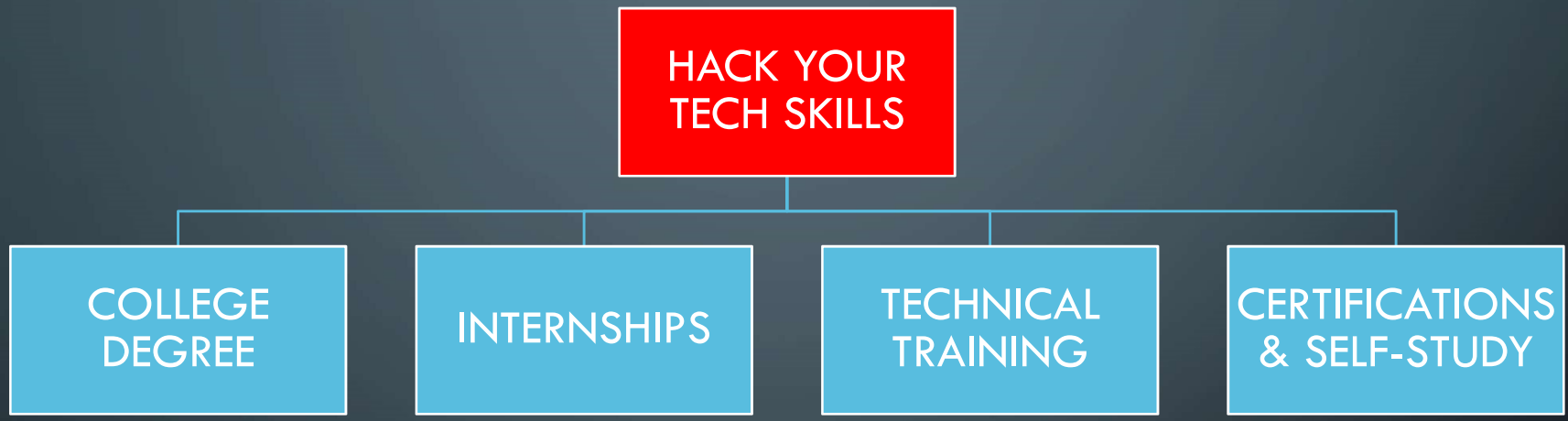
https://www.csoonline.com/article/3247667/demand-for-cybersecurity-talent-rises-sharply.html

So…what can I do to get my foot in the door?

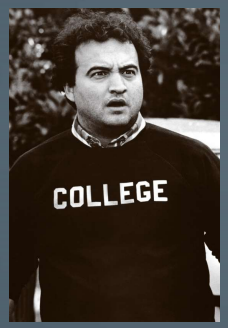
GETTING HIRED – MULTI-LAYER APPROACH



GETTING HIRED - HACK YOUR TECH SKILLS



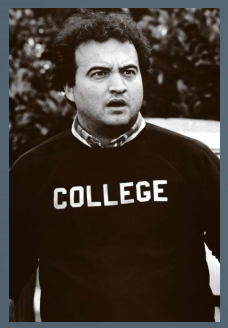
COLLEGE DEGREE



- PROS
  - Formal, recognized education
  - Provides a general technical foundation
  - Builds soft skills (time management, communication, writing skills, etc.)
  - Future higher learning (Master's, PhD)
- CONS
  - Expensive, competitive
  - 2-5+ years to complete depending on background/availability
  - Student/employer skills gap

- Not a prerequisite for all employers, but it is for many
- Not right for everyone, adjust accordingly

COLLEGE DEGREE



- General CS/CE Degrees (4 yr)
  - WSU/UW
  - University of Oregon
  - OSU
  - PSU
  - University of Portland
- Specialized Cybersecurity Degrees (4 yr)
  - UMUC
  - WGU
  - Utica
  - Drexel
  - Purdue University Global
- AA/Certificate (1-2 yr)
  - Mt. Hood Community College – AAS CyberSecurity and Networking
  - Portland Community College – Cybersecurity Fundamentals Certificate

INTERNSHIPS

- PROS
  - Can be very high quality experiences
  - Realistic experience prior to seeking your first security job
  - Possible intern-to-hire path
- CONS
  - Can be very low quality experiences
  - No job guarantee
  - Might be short term

- Single biggest thing college students can do while still in college
- Make the most of it so employers don't look at you as "inexperienced"
- Seek multiple

INTERNSHIPS

- Alternative Programs Exist
  - Some organizations are starting to adopt creative approaches to traditional internships
  - NetSPI-U
    - Helped us build quality entry-level talent
    - Offered graduating students a full-time, paid job with benefits and extensive training
    - Helps fill hiring pipeline rather than always relying on trying to find qualified candidates in the job market

TECHNICAL TRAINING

- PROS
  - Formal, structured learning
  - Foundation in a specific technical area
  - Taught/offered by experts
  - Costs less than the college
- CONS
  - Quality can vary
  - Employers may not consider it a substitute for a degree
  - Crash course that isn't necessarily mastered by the participants right away

- Build specific skills/learn specific tools while holding down your day job
- Good for mid-career professionals to pivot into the InfoSec industry

TECHNICAL TRAINING

- Black Hat Trainings
- SANS Courses
- Offensive Security Courses
- Splunk
- Coursera
- Portland OWASP Training Day
- Microsoft Training
- AWS Training
- Cisco Training
- Puppet
- Udemy

List goes on and on…

CERTIFICATIONS

- PROS
  - Shows competency in specific areas
  - Short-ish timeframe to complete
  - Good addition for all skill level
- CONS
  - Reputation can vary…do your research
  - Certs != jobs
  - Can be overwhelming and unstructured if you choose to self-study

- Shows employers you're dedicated to learning and building your skills
- Offset some* experience shortcomings

CERTIFICATIONS

- Generalized
  - GIAC Security Essentials (GSEC)
  - CompTIA Security+
- Networking
  - CompTIA Network+
  - Cisco CCENT (Entry Network Tech)
- Penetration Testing
  - eLearnSecurity Penetration Testing Student (PTS)
  - CompTIA PenTest+
  - OffSec (OSCP)
- Cloud
  - AWS CCP (Cloud Practitioner)
  - MS Certified Azure Fundamentals

SELF-STUDY

- PROS
  - Completely at your own pace
  - Focus on what you want to learn
  - Saves $$$ on training courses if studying for a cert
- CONS
  - Difficult to find motivation at times
  - No schedule or deliverables
  - Lacks structure and can be overwhelming

- Great way to ease into InfoSec and explore its many corners
- Where to start? Let's find out…

SELF-STUDY

- PRACTICE RESOURCES
  - Hack the Box: https://www.hackthebox.eu/
  - VulnHub: https://www.vulnhub.com/
  - OWASP Juice Shop: https://www.owasp.org/index.php/OWASP_Juice_Shop_Project
  - OWASP WebGoat: https://www.owasp.org/index.php/Category:OWASP_WebGoat_ProjectVulnHub
  - Damn Vulnerable Web App (DVWA): http://www.dvwa.co.uk/
  - Rapid7 Metasploitable: https://github.com/rapid7/metasploitable3

SELF-STUDY

- BUILD A HOME LAB
  - Get an old server, install VMware ESXi, and start building practice VMs
  - Any moderately powerful modern day computer will run a couple of VMs in VirtualBox to practice with
  - r/homelab
  - Turnkey Linux - https://www.turnkeylinux.org/

SELF-STUDY

- CTFs (Capture the Flag)
  - CTFtime: https://ctftime.org/
  - SANS Holiday Hack: https://www.holidayhackchallenge.com/
  - Every CTF is different, but they generally contain a variety of categories to cater to all aspects of security:
    - Web app
    - Network
    - Forensics
    - CrackMe/Pwnables
  - Write-ups posted by top teams, so if you struggle you can find the solution after the CTF is over

SELF-STUDY

- Some of my favorite books to get you started in AppSec/PenTesting
  - RTFM: Red Team Field Manual (B. Clark)
  - The Hacker Playbook (1, 2, & 3) (P. Kim)
  - Penetration Testing (G. Weidman)
  - Black Hat Python (J. Seitz)
  - Violent Python (T. O'Connor)
- Oldies, but Goodies:
  - The Web Application Hacker's Handbook (2nd Ed.) (Stuttard/Pinto)
  - Hacking Exposed 7 (McClure/Scambray/Kurtz)

SELF-STUDY

- Some of my favorite news sources to get you started in InfoSec:
  - Reddit
    - r/netsec
    - r/netsecstudents
    - r/asknetsec
    - r/security
    - r/sysadmin
  - Twitter (keep an eye out for blog authors and speakers that interest you)

GETTING HIRED – MULTI-LAYER APPROACH

PROFESSIONAL NETWORK

- Building your professional network requires that you be….professional.
- Online Networking:
  - Employers will search out your social media profiles
  - Set as much as you can to private
  - You have a life outside of work, but remember that the initial hiring process is hard, so try not to have anything working against you
  - Keep your LinkedIn profile polished and up-to-date
  - Connect with relevant security contacts

PROFESSIONAL NETWORK

- Local Networking
  - LOTS of opportunities here in PDX for local networking!
    - Conferences
    - Security Meetups
    - Hackerspaces

PORTLAND SECURITY CONFERENCES

https://bsidespdx.org

https://www.linkedin.com/company/bsidespdx/

@BSidesPDX

- BSides PDX
  - Annual security conference held in Portland (October-ish)
  - 2-day event featuring security talks from both novices and experts, hands on learning opportunities (CTFs, training), and some local sponsors/vendors
  - Inexpensive (various price levels - free, T-Shirt ($10), Patron ($100), name your price)
  - Growing every year

PORTLAND SECURITY MEETUPS

https://www.owasp.org/index.php/Portland

https://www.meetup.com/OWASP-Portland-Chapter/

https://www.linkedin.com/groups/4223013/

@PortlandOWASP

- Portland OWASP Chapter
  - Monthly meetings around PDX
  - Both technical and non-technical topics
  - Lots of variation in experience levels of attendees (great for newcomers!)
  - Caligator Event Page - Speakers/Events
    http://calagator.org/events/search?query=OWASP
  - 2019 OWASP Portland Training Day
    https://www.owasp.org/index.php/OWASP_Portland_2019_Training_Day

PORTLAND SECURITY MEETUPS

https://www.meetup.com/RainSec/

@PDXRainSec

- Portland RainSec
  - Last Tuesday of the month @ Wedgehead (NE Sandy)
  - Informal security discussion and professional networking over beers
  - Variety of experience levels, from complete novice to seasoned experts
  - Welcoming atmosphere for newcomers…meet some people!

PORTLAND SECURITY MEETUPS

http://www.pdx2600.org/

@PDX2600

- Portland 2600
  - First Friday of the month - 7pm @ Theo's (NW 5th Ave.)
  - Related to the 2600 Hacker Quarterly publication
  - Open to anyone regardless of age or skill level
  - Smaller crowd, more opportunity for 1-on-1 conversations
  - Main Page is outdated - check on Twitter for news/details
  - Can also check 2600 Meeting List - Details for all 2600 meetings worldwide https://www.2600.com/meetings/mtg.html

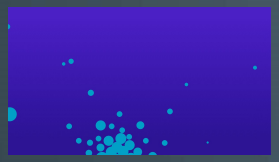
PORTLAND SECURITY MEETUPS

http://503.ninja/

@DC503

- DC503 - Portland DEF CON Group
  - Third Sunday of the month - 3pm @ Undisclosed Location (ask around)
  - This meetup is, generally speaking, not for novices. You are expected to participate and present. Think about attending down the line or when you have some interesting research to present.

~~PORTLAND~~ VANCOUVER SECURITY MEETUPS



https://www.meetup.com/Vancouver-Digital-Security-Meetup/

- Vancouver Digital Security Meetup
  - Meets twice per month (one AM and one PM meeting)
  - Branch of the larger Vancouver-based VenTechy Meetup group
  - Informal security discussions and networking over bagels (AM) or beers (PM)
  - Welcoming atmosphere for newcomers

PORTLAND HACKERSPACES

https://pdxhackerspace.org/

https://www.meetup.com/CTRL-H/

@ctrlhpdx

- ^H (CTRL-H)
  - Creative hacker/maker space for a variety of tech-influenced projects
  - 24/7 access for general purpose use – other special areas also exist such as a wood shop, electronics lab, and craft lab via reservation
  - Think 3D printers, soldering irons, oscilloscopes & other nifty tools you might not have
  - Membership ($40/mo) – they host weekly open houses (usually Thursday nights) to come check it out
  - Exploit Workshop – Wednesday nights devoted to computer security, exploit development, research, some presentations (no membership required)

PORTLAND HACKERSPACES

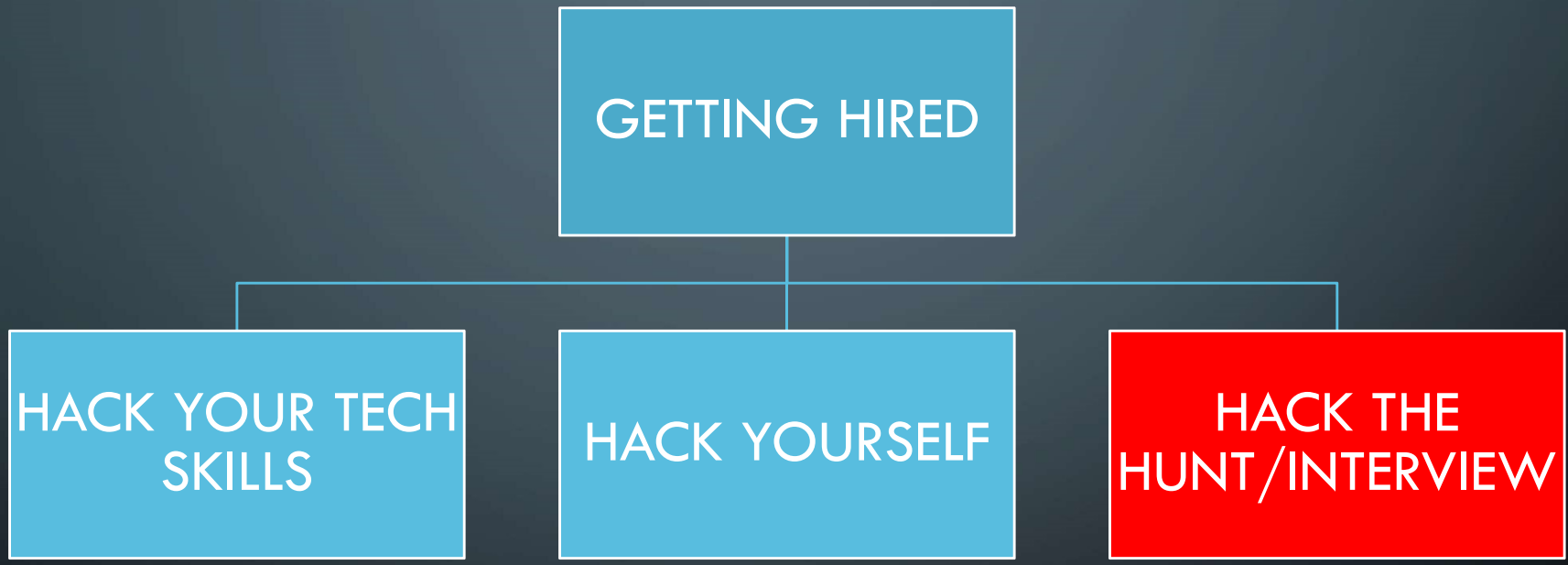
https://www.pascalpdx.org

https://www.meetup.com/pascalhackerspace/

@pascalpdx

- PASCAL
  - Portland Area Scientific and Cultural Advancement League
  - Non-profit serving the InfoSec community
  - Membership (?/mo) for 24/7 access – they host open houses to come check it out
  - InfoSec related events, check the calendar

GETTING HIRED – MULTI-LAYER APPROACH



GETTING HIRED – MULTI-LAYER APPROACH

THE RÉSUMÉ

- Be honest and accurate
  - Anything on your résumé is fair game in an interview
- Tailor every résumé to the company and position
- If you're slightly experienced, focus on past achievements opposed to listing skills
- If you're inexperienced, focus on side projects, relevant volunteer work, CTF participation, etc.
  - Anything that shows you're interested in security and are doing something with it

THE RESUME

- Find someone in the InfoSec community to review your resume
- SPELL.CHECK. Pretty please?
- SurferGal22@aol.com and similar are not ok
- Use the cover letter to provide context to the reviewers
- Include LinkedIn profile link

JOB SEARCHING - BOARDS

- Lots of options to choose from, but some of the more popular:
  - Indeed - https://www.indeed.com
  - LinkedIn Jobs - https://www.linkedin.com/jobs
  - Glassdoor - https://www.glassdoor.com
  - Reddit r/netsec Quarterly Hiring Thread - https://www.reddit.com/r/netsec
  - College job boards
- Target entry-level positions even if you don't meet the experience reqs
- Referrals/recommendations really help

THE INTERVIEW

- Every company will handle the process differently
- Typical?
  - Phone screen with HR/hiring manager
  - Phone interview with a team resource (mid to senior level co-worker)
  - Phone interview with a team lead/manager (your boss)
  - On-site
    - Face-to-face interviews with other teammates or managers
    - Hands-on technical assessment

THE INTERVIEW

- Phone screen with HR/hiring manager
  - First impression…dazzle them
  - Be honest, clear, and enthusiastic
  - They're looking for a minimum set of criteria to pass you to the next phase, usually:
    - Very basic tech screen
    - Salary requirements
    - Criminal history/issues that might prevent hiring (non-compete, etc.)
- PURPOSE: Make sure you could potentially complete the hiring process

THE INTERVIEW

- Phone interview with a team resources (mid to senior level co-worker)
  - First technical portion
  - Fairly easy questions that progress in difficulty
  - Be prepared, know your stuff
  - It's OK to not know something, just say so
- PURPOSE: Make sure you possess at the minimum technical baseline required to perform the job duties

THE INTERVIEW

- Phone interview with a team lead/manager
  - Could be less technical, but not always
  - If technical, they'll try to dig deeper than previous round
  - If not technical, they'll be talking to you more about how you handle things like:
    - Deadlines
    - Stress
    - Problems in the workplace
- PURPOSE: Make sure you meet the technical criteria and are going to be a good fit for the team from a personality and managerial perspective

THE INTERVIEW

- On-site
  - Final step
  - Opportunity for YOU to meet the team/ask questions/check out workplace
  - A good hiring process will ask you to demonstrate hands-on technical skills
  - Extent of hands-on may vary depending on skill level and job requirements
- PURPOSE: Make sure you can technically execute all of the things you were able to talk about on the phone. Confirm personality fit.

CELEBRATE!

FINAL THOUGHTS

- There is no “right” way to get into InfoSec
- Think outside of the box
- Be persistent and dedicated, it will happen
- Be an InfoSec champion in your daily life

QUESTIONS?