So, you want a career in Security?

Derek Hill
Sr. Director Software Engineering – Application Security
ForgeRock Inc. (now Ping Identity)
@secureITtoday
https://www.linkedin.com/in/derekphill/
derek@dh-solutions.com or derek.hill@forgerock.com

What to expect

- Just a few slides
- I encourage lots of interaction and questions
    - I might defer a question until a later slide
    - There are no stupid questions
- This is not an interview, so don’t be afraid to ask things you wanted to know, but didn’t know how to ask

Lot of jobs (today and in the future)

- Security had a projected global shortage of about 3.5 million people (750k in the US alone) in 2025 - https://cybersecurityventures.com/jobs/
- It is a very big field (almost like healthcare, not size but scope)
  - Many different types of roles …. Just some examples
  - Blue team
  - Red team (or blended → Purple team)
  - Auditing
  - GRC (Governance, Risk, Compliance)
  - Security Operations Center (SOC) – considered the entry role by many
  - Etc.....
- Shortage is not only bodies, but also skills

How to get ready for that job

- Think about what exactly you want to do
    - Talk to friends, teachers, industry professionals and see what interests you
- Spend some time in various security groups (even Reddit)
    - Get exposed to what is out there in terms of vulnerabilities, what people are working on, etc
    - Lots of great local security groups to participate in
        - Some paid (ISSA, ISACA)
        - Lots of free (OWASP [membership optional], CTRL-H, DefCon 503, Vancouver Security meetup, 2600, RainSec, etc)
        - Make connections, learn what others are working on, topics of the day/week, etc
        - Go to DefCon ($440 for the ticket, but you have to get to and stay in Vegas)
- Once you figure out what you want to do, spend extra time getting ready
    - Education in school is great, but that really only scratches the surface
    - Pursue internships, volunteer, anything to get some real world experience
    - Additional security specific education/certifications – a great “lower cost” certification is OSCP
    - Participate in security events such as Capture the Flag (CTF), and other free training
    - Enroll with one or more bug bounty programs and try out your skills, you could even earn some money (HackerOne or BugCrowd)
- Be passionate

You have experience – even if you don’t realize it

Quote from the article: https://cybersecurityventures.com/jobs/

> *Despite the disarray of the tech industry, cybersecurity remains a near-zero unemployment marketplace for those with extensive backgrounds, and the shortage means that IT teams must also shoulder a security burden. Staff must train in modern threat awareness, including phishing, social engineering, Business Email Compromise (BEC), and financial fraud. They must also know how to protect and defend apps, data, devices, infrastructure, and people.*

- Every IT position is also a cybersecurity position now. Every IT worker, every technology worker, is (or should be) involved at some level with protecting and defending apps, data, devices, infrastructure, and people.
- A rticulate your experience on your resume AND cover letter(s)……..you do have a cover letter, right?

What about my team(s)? – past & present

- Over the years, I have managed a variety of security teams, skills/experience(s) vary drastically, some examples:
- Application Security (purple team)
  - Be able to read and write code
  - Spot vulnerabilities in code
  - Background CS major with a security focus/interest
  - Curious, want to figure out a way to break stuff
- Infrastructure Security and Compliance (blue team)
  - Defense, secure the infrastructure that houses the applications and data
  - System admin background
  - Scripting or programming background
  - Automate things as much as possible, think infrastructure as code
  - Report on security findings and communicate to stakeholders
- Governance, Risk Management & Compliance (GRC)
  - Creating and updating policies, required for certifications such as ISO
  - Processes and risk acceptance
  - Measuring for effectiveness (auditing)
- Data Privacy Engineering
  - Ensure we are doing the right thing, only collect what we need, don't keep it any longer than we need & protect it adequately
  - Privacy by Design and Privacy by Default
  - Comply with regulations all around the world
  - Focus is on GDPR (EU), Data Protection Act (UK), CCPA (California) and the various spinoffs (countries and states)

Lots of other roles out there

- Pen Tester
- Reverse exploit researcher
- Hacker for the mob or the government
- Professional bug bounty researcher
    - Yes, people specialize in certain types of vulnerabilities and become experts (small but very specialized scope, great potential)
- Auditor
- Security Operations
- Incident Handling / Response
- Forensics
- and many more

It comes back to passion and pursuing it

……and when all else fails, there is always management

Resources

just a few examples, lots more out there

- Local training and meetups (not only security): http://calagator.org/
- Security "meetups": https://www.meetup.com/find/?allMeetups=false&radius=25&userFreeform=98683&mcId=z98683&keywords=security&source=EVENTS&location=us--or--Portland
- RainSec: https://www.meetup.com/rainsec/
- OWASP security training (webgoat): https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- Damn Vulnerable Web Application: https://github.com/digininja/DVWA
- PDX Hackerspace (CTRL H): http://pdxhackerspace.org/
- Portland 2600: http://www.pdx2600.org/
- CTF Events: search for "free CTF events" – lots of them out there, a personal favorite is the SANS holiday hack challenge: https://www.holidayhackchallenge.com/2022/
- Pentesting with Kali (PwK) and OSCP certification: https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/