A Guide Getting Started with Cybersecurity

@linux_girl

04/06/2021

DISCLAIMER

The views, thoughts and opinions expressed in this presentation belong solely to the author and not necessarily to the author's employer, organization, committee or other group or individual


STOP
ASIAN
HATE

A VERY PROUD CAL POLY ALUMNI!

Spent hours in this library!

Credit: ttps://www.freepik.com/photos/background'>Background photo created by jcomp - www.freepik.com

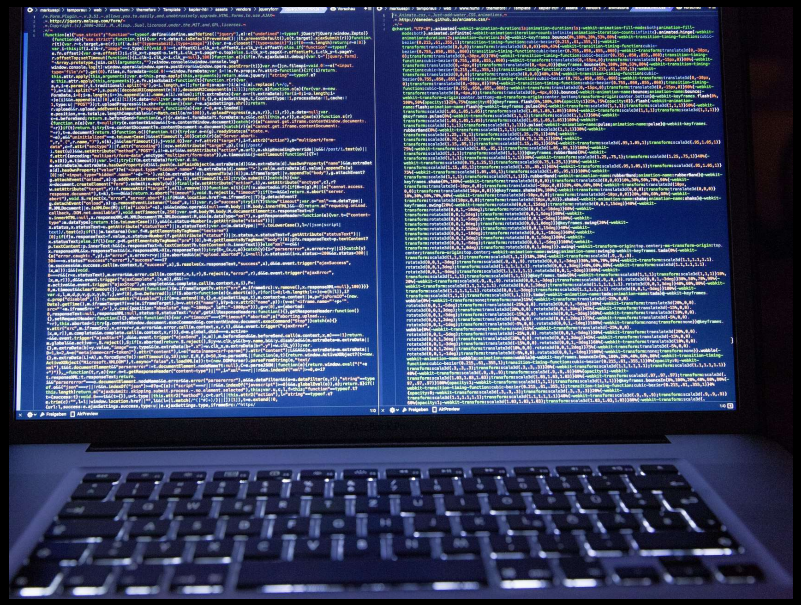
Source: https://commons.wikimedia.org/wiki/File:Calpoly_pomona_university_library.jpg

WHY GETTING STARTED IN CYBERSECURITY?

- Zero Percent Unemployment
- Unlimited Growth
- Plenty of Variety of Fields
- Solve Puzzles

WHY GETTING STARTED IN CYBERSECURITY?

- Competitive salary
- Can hack things and get paid
- Bleeding edge technologies
- Satisfaction when you break into a system successfully



FINDING AN ENTRY LEVEL JOB

- NOT EASY!
- Very Competitive !

https://pixabay.com/photos/women-running-race-racing-athletes-655353/

EVEN ENTRY LEVEL JOBS……

- 3-5 years of experience
- Degrees (CIS, CS, engineering and STEM)
- Certifications

Credit: https://www.careeraddict.com/uploads/article/55295/work-experience-note-pinboard.jpg
Credit: http://www.solano.edu/degrees/images/bnr_degrees_certificates.jpg

FEEDER ROLES INTO ENTRY-LEVEL CYBER JOBS

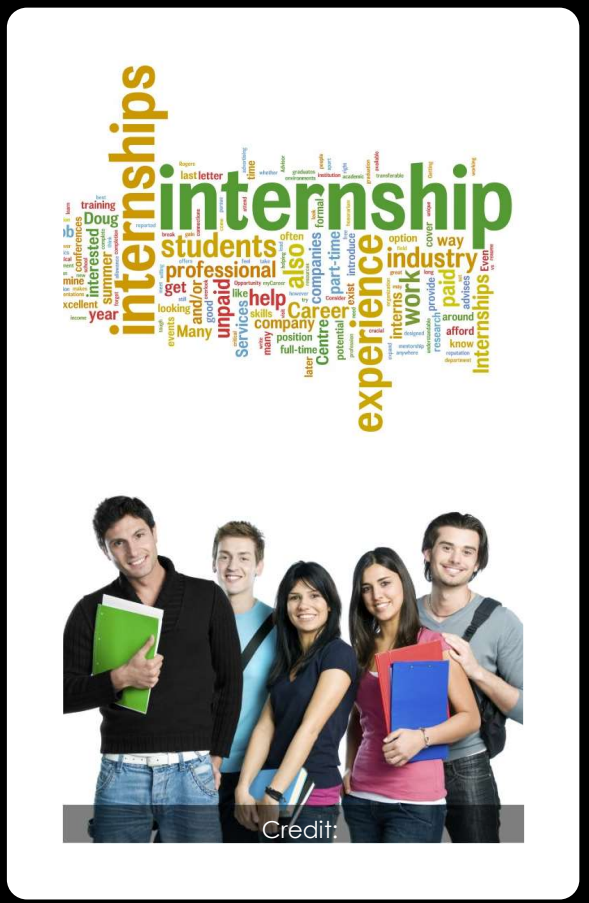
- Feeder Roles
  - Network Engineer
  - Systems Engineer
  - System Administrator
  - Software Developer
  - Help Desk Technician

It is NOT ABOUT YOUR JOB TITLE!!!

Credit: https://asmithblog.com/wp-content/uploads/2016/07/strengths-job-title-titles.png

AN INTERNSHIP CAN LAND YOUR NEXT JOB!

- #1 Recommendation for university students:
  - FIND AN INTERNSHIP!
  - Even if it is far away or in a boring city
  - It is usually about 12 weeks – NOT FOREVER
  - It is totally worth it (start when you are a freshman)



https://www.biginternships.com/freshman-internships


Cyber Security Tools
www.educba.com


BANK


Insurance


CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA


Sports

INTERNSHIP CANDIDATES SELECTION PROCESS

- **Well, it depends .....**
- **Large corporations**
  - GPA
  - Key words (might use a resume scanner software, before a resume reaches to a recruiter)
  - Multiple levels
    - Recruiter → Hiring Manager
- **Smaller companies**
  - Can reach out to the hiring manager directly

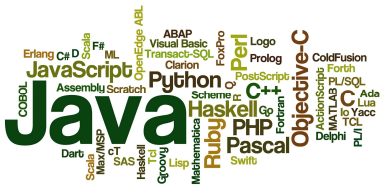
WHAT HIRING MANAGERS ARE LOOKING FOR

- Basic understanding of what cybersecurity is
- Think critically, problem solve and work independently
- Teachable
- Work well with others
- Have a passion for cybersecurity (not just looking for a high paycheck)
- Everything else I'll teach you

FOUR SKILLS

- Networking
- Linux
- Programming Language
- Soft Skills

**Many free resources are there. Especially during covid, the training classes are either free or very low cost



MAKE YOURSELF STANDOUT

- Build a home lab
- Start a blog
  - Write about what you are working on and why/what inspires you
- Get into Capture the Flag (CTF)
- Build a GitHub/GitLab repository
- Contribute to an open source project
- Volunteer at a cybersecurity conference / meetup
- Speak the language (through understanding)
- Doing unpaid internship

Basic Security Home Lab - with Charles Judd

BUILD YOUR PROFESSIONAL NETWORK

- Local security meetups and organizations
  - **In-Person**
  - Virtual
- Conferences and trainings
- Social Media

Credit:
https://www.insidehighered.com/sites/default/server_files/media/networking.jpg

BUILD A STRONG NETWORK

1. Right People
2. Win/win Situations
3. Give Before You Receive

FIND A MENTOR

STRATEGIES FOR EFFECTIVE

MENTOR MENTEE RELATIONSHIP

01 COMMIT TO EACH OTHER

02 DEVELOP TRUST

03 PLAN GOALS

04 ROLES AND RESPONSIBILITIES

05 COLLABORATE FOR RESULTS

Credit:
https://keynotesbh.com/wp-content/uploads/2017/08/mentorshi2.jpg

STAY SAFE !

Source:
https://www.thedoctorstv.com/articles/how-does-coronavirus-covid-19-affect-your-petS

Credit: https://pixabay.com/photos/arrow-books-hand-keep-direction-3029370/

Source: https://pixabay.com/illustrations/thank-you-letters-140227/

Source: https://pixabay.com/illustrations/question-question [illegible] quest-63916/

BACKUP SLIDES

CYBERSECURITY ROLES

Hands-On Roles

- Application Security Engineer
- Cloud Security Engineer
- Cyber Data Scientist
- Cyber Insider Threat Analyst
- Cyber Risk Analyst
- Cyber Threat Intelligence Analyst
- Cybersecurity Administrator
- Cybersecurity Advisor

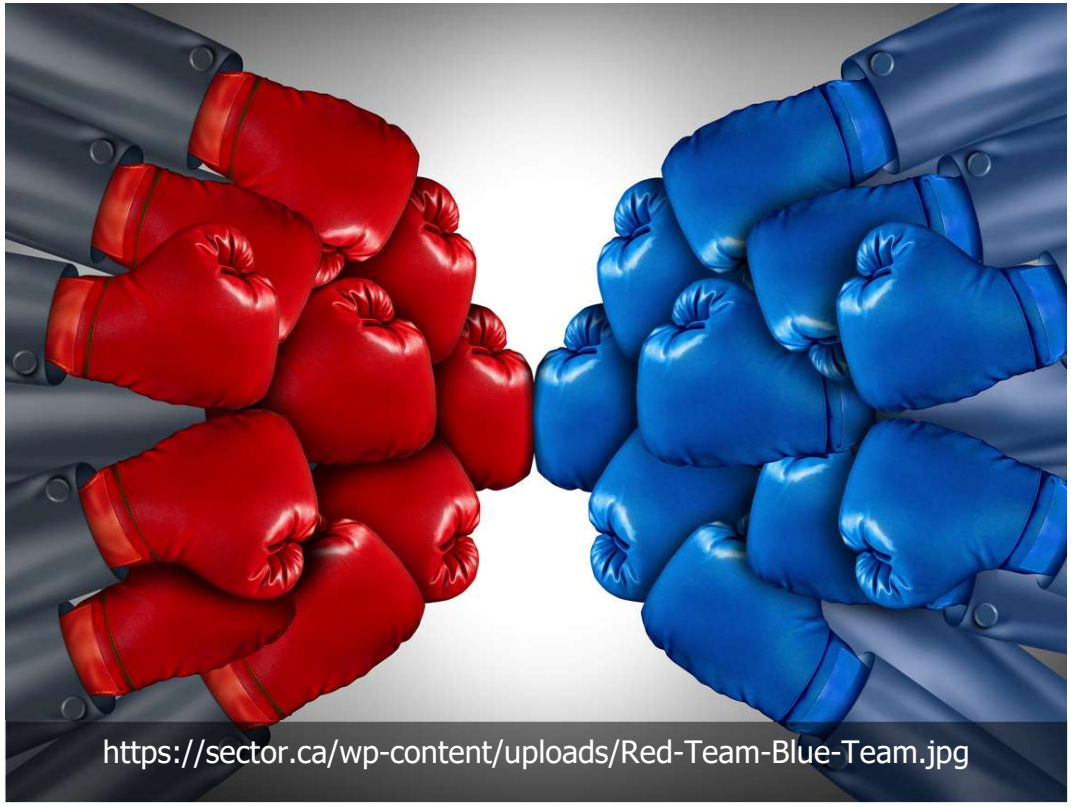
https://www.cybersn.com/cybersecurity-job-categories

- Cybersecurity Advisor
- Cybersecurity Forensics Analyst
- Cybersecurity Intern
- Cybersecurity Sales Engineer
- Cybersecurity Software Engineer
- Cybersecurity Specialist
- Data Loss Prevention Engineer
- Data Security Engineer
- DevSecOps
- Governace & Compliance Analyst
- Identity And Access Management Engineer
- Incident Responder

Source: https://niccs.cisa.gov/formal-education/students-launch-your-cyber-career

ROLES OF RED, BLUE AND PURPLE TEAMS

- Red Team
  - Attack
- Blue Team
  - Defend
- Purple Team
  - Support the process



https://sector.ca/wp-content/uploads/Red-Team-Blue-Team.jpg

RED TEAM ROLE

- Typically, an external team, that hired to test its defenses
- Deploy bleeding edge hacking tools and techniques to infiltrate systems and premises
  - Could extend to writing their own malware
- Traditional penetration testing

RED TEAM METHODS

- Initial Reconnaissance
- Deploy command-and-control servers (C&C or C2) to establish communication with the target's network
- Use decoys to throw the blue team off the scent
- Apply social engineering and phishing techniques

RED TEAM OBJECTIVES AND DUTIES

- Compromise the target's security
  - Extracting information, infiltrating its systems or breaching its physical perimeters
- Avoid detection by the blue team
- Exploit bugs and weakness in the target's infrastructure
- Initiate hostile activity

BLUE TEAM ROLE

- Understand every phase of an incident response
- Notice suspicious traffic patterns and identifying indicators of compromise
- Rapidly shutting down any form of compromise
- Identify the threat actor's command and control (C&C or C2) servers and blocking their connectivity to the target
- Undertake analysis and forensic testing on the different operating systems (including use of third-party systems)

BLUE TEAM METHODS

- Review and analyze log data
- Use a security information and event management (SIEM) platform for detection of live instructions and to triage alarms in real-time
- Gather new threat information
- Perform traffic and data flow analysis

PURPLE TEAM

- Not a permanent team
- Oversee and optimize the red and blue team exercise
- Typically – security analysts or senior security personnel
- If the red and blue teams work well – a purple may become redundant

WHAT YOU NEED TO LEARN

- How computer works **
- Virtualization
  - Build your home lab
- Linux
  - Cybersecurity or hacking distribution is based on Linux (there is now way around it)
- Networking
- Firewall
- Windows Server and domains
  - Each company will run some kind of Active Directory. Windows still being the most dominate
- Install your first security Linux distributions
- Capture the Flag (essential part learning cybersecurity) – permanently working on a CTF


HOW TO GAIN CREDIBILITY WHEN YOU HAVE LITTLE EXPERIENCE
We are looking for someone age 22-26 …. With 15 years of experience ☺

RESOURCES:

Videos

- How to Start a Career in Cyber Security with the Cyber Mentor
- How to Get Into Cybersecurity with No Experience
- 5 Entry Level Cyber Jobs You Need to Know About