CAREER, CERTIFICATIONS, & COMPETITIONS (C^3)

Taylor Kaufman, CISSP

ABOUT ME

- Current Role
  - Risk Process Technical Specialist, M&T Bank
    - Banking Officer,
  - CISSP, Network+, Security+ certified
- Previous roles
  - 2.5 years as a Security Engineer, Seneca Gaming
  - 1 year IT support technician, Seneca Gaming
- Personal
  - Graduated Buffalo State College class of 2015
    - B.S. Computer Information Systems
    - B.A. Television/Film arts
    - Minor, Philosophy
  - InfraGard Buffalo and Technology advisory board member for the town of Grand Island
  - Amateur boxer out of Casal's boxing club
  - Cybersecurity/Information Security nerd

CAREER

- Started out on IT support working overnights
  - Learned troubleshooting hardware, software, networking, systems, DBA, etc.
  - Was very interested in cybersecurity, asked to shadow the ISA (Information Security and Assurance group) after my normal Midnight to 8am shift
  - Assisted on overnight/off hours upgrades such as Firewall upgrades, Content filter upgrades, etc.
- Transitioned to Security Engineering after obtaining Network+ and Security+
  - Learned about anti-virus software, firewalls, content filters, SIEM rules, incident response, identity and access management, encryption, etc.
- Current position as a Cybersecurity Risk Process Technical Specialist
  - Designing, automating, and building more efficient processes in vulnerability risk management
  - Designing new processes and procedures for new technologies such as Cloud, Containers, etc.
  - Less hands on, more of a hybrid between architecture/design, project management, risk management

CAREER

Entertainment

- 24/7, 365 operations
- Less regulation
- 5 properties (3 casinos, 1 golf course, 1 corporate building), only NY state
- Needed to know a lot about a variety of things, was responsible for everything from firewalls to anti-virus to policies to SIEM, etc.

Finance

- 24/7, 365 operations
- Highly regulated
- 780+ branches, numerous corporate buildings, spans several states/countries
- A lot of division of specialties between groups. Example: One team handles Firewalls, one team handles the SIEM, etc. Separation of duties

CERTIFICATIONS

Beginner Certifications

- **CompTIA**
  - No experience necessary
  - Relatively cheap to pay for out of pocket ($200+), cheaper maintenance fees
  - CompTIA requires 3 year recertification with CEUs (Continuing education units)
  - Range of various subjects (networking, security, pentesting, Linux, etc.)
  - Stackable for extra titles

- **Microsoft/Google/Amazon**
  - No experience necessary
  - Relatively cheap to pay for out of pocket ($50+)
  - Microsoft Cloud certifications such as Azure Fundamentals, AWS are in high demand
  - Range of various subjects (Cloud, developer, operations, etc.)

CERTIFICATIONS

Advanced Certifications

- All of these are highly desirable certifications due to the experience necessary to obtain them

- **(ISC)²**
  - Need to have years of 'real world' experience to obtain full certification. Pass an exam and prove experience to be fully certified
  - Expensive to take exams ($700+), and expensive maintenance fees ($120/yr)
  - CISSP requires 5 years of cumulative experience in two of eight domains of the CBK
  - Requires 120 hours of Continuing education credits over three years
- **ISACA**
  - Certifications are more in the cybersecurity risk, incident handling, and governance domains
  - Can be expensive to take exams ($575/member, $760 non-member), but cheaper maintenance fees ($45/yr. member/$85 non-member)
  - Certifications typically require 3 years of cumulative paid experience in two of four domains of the CBK
- **Offensive Security**
  - Need to be hands on knowledgeable in systems, exploits, penetration testing
  - Can be expensive ($1000+ for labs and examination)
  - OSCP is most notable

COMPETITIONS – CTF 101

- CTF (Capture the Flag) is a kind of information security competition that challenges contestants to solve a variety of tasks to find a specific piece of text that may be hidden on the server or behind a webpage. This goal is called the flag.
- Example of a typical flag format:
  CTF{Th1s1s@Fl@g!!kl23$#s}
- The very first cyber security CTF developed and hosted was in 1996 at DEFCON in Las Vegas, Nevada.
- Can be held on site or online and can be played as an individual or in teams.
- Major events such as Google CTF, Defcon CTF, HITB, etc. all offer major monetary prizes and exposure for security professionals who compete.

TYPES OF CTF AND CATEGORIES

- Three main CTF event styles:
  - Attack-Defense
    - Defend a host PC while trying to attack an opposing team's PC
    - You get points for staving off attacks and infiltrating other teams
  - Jeopardy CTF
    - Presented with clues which guide in completing specific tasks to find a flag
    - Points are earned based on completion
  - Mixed events

- Categories for CTF include (but are not limited to):
  - RE (reverse engineering): get a binary, reverse it to find a flag
  - PWN: bypass normal functionality on an endpoint to read a flag
  - Crypto: get an encrypted file and learn how to decrypt for the flag
  - Web: exploit web vulnerabilities (SQL injection, XSS, etc.) to find the flag
  - Forensics/Stego: PCAP files, image, audio, etc. hide a flag
  - Other: Puzzles, OSINT, electronics based, etc.

THIS SOUNDS INTERESTING, WHERE DO I START?

- Commonly used tools:
  - OS such as BlackArch, Parrot, or Kali Linux
  - Binwalk – extract and analyze files
  - Burp suite – web pent tools
  - Stegsolve – for finding anything hidden within images, etc. (steganography)
  - IDA – reverse engineering
  - COMMAND LINE!!!
  - Big breakdown guide here: https://github.com/apsdehal/awesome-ctf
  - Owning a dark hoodie never hurt

- Entry level practice sites:
  - PicoCTF – originally designed for middle schoolers and high schoolers, you don't need to download any tools. All done through web.
  - CTFlearn.com – various collected challenges aimed towards newcomers
  - Overthewire.org/wargames and hackthebox – connect to games via SSH (like putty) and use tools on your own machine to try these challenges
    - Please note: there are a lot of established write ups for these challenges. If you wish to work through them yourselves, make sure to avoid youtube or git repositories with them

I HAVE SKILLS NOW, SO WHERE DO I FIND EVENTS?

- CTF Time and CapCTF calendar for event listings
- Infosec Conferences
- Security and Technology institutes and companies such as SANs, GIAC, Synack, Cisco, and Google
  - **CyberReason is currently accepting registrations for their virtual CTF (Aug 19th- 24th)**
- Discord, Twitter, Reddit/r/netsec or Reddit/r/securityCTF
  - Following established CTF teams are a good way to find information on their next events (ex. Perfect blue, Defenit, OpenToAll, More Smoked Leet Chicken, ARESx etc.)
  - These are also good places to search for or start your own team for events

ARESx

QUESTIONS?

- Taylorannekaufman@gmail.com
- https://www.linkedin.com/in/taylorannekaufman/