**TRUSTEDSEC**

**INFORMATION SECURITY +**
**ADVISORY SERVICES CONSULTING**

Creating Your Career Path in Information Security

# Agenda

- Introductions
- Understanding common roles
- Picking your path
- Where to gain knowledge
- How to present yourself
- Q & A's

# OUR MISSION

TrustedSec is an information security consulting team at the **forefront of attack simulations** with a **focus on strategic risk-management**.

Our goal is to help organizations defend against threats of all kinds and **change the security industry for the better.**

# How we approach security differently.

## AT THE FOREFRONT

Senior-level consultants;
Adversary Emulation, Threat & Research team;
Develop widely-used open source tools

## INTEGRATED RISK MANAGERS

Deep experience in advisory practice;
Dedicated to improving overall security posture;
Established industry regulatory standards

## A PARTNER AND A FRIEND

Commited to improving the state of security;
Creator of DerbyCon;
Assist in incident and breach responses

# RESEARCH AT THE FOREFRONT

At TrustedSec, we believe in the value of gaining and sharing knowledge. Our Adversary Emulation, Threat & Research (AETR) team is solely dedicated to researching the best ways to serve our clients while continually advancing our own expertise.

*"Through research, we're gaining knowledge and using it. Our custom tooling is not going to be off-the-shelf—it's more effective, stealthy, and an overall better simulation of an adversary."*

*—Carlos Perez, Practice Lead, Research & Development*

- Tactics, techniques and procedures development

- Expands team's tool sets and investigates novel threats

- Works directly with TrustedSec Red Team and Incident Response Team

- Lead renowned tactical instructor and researcher Carlos Perez

# TRUSTEDSEC TECHNICAL AND ADVISORY SERVICE OFFERINGS

**Network Penetration Testing**
**Incident Response**
**Social Engineering**
**Software Security Testing**
**Hardware Security Assessments**
**Red/Purple Team**
**Risk Assessments**
**PCI/GDPR/HIPAA Compliance**
**Framework Alignment**
**Attack Path Coverage Assessments**
**Program Maturity Assessments**
**Virtual CSO**
**Employee Training**

# Adam Compton

## Senior Security Consultant

Over my life, I have been a programmer, researcher, instructor, professional pen tester, father, husband, and farmer.

I have nearly two decades of experience in the Information Security field performing programming, network security, incident response, security assessment, and penetration testing.

# Tyler Hudak

Practice Lead, Incident Response

I have almost 20 years of experience in information security and have had multiple roles, including on the red team and in incident response (my current passion).

I love to share my knowledge in conferences and in my training with the hopes that others can benefit from what I've learned.

**Education & Certifications -**
BS Computer Science, University of Akron, GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE)

# How did Adam get here?

- I got a computer (Commodore 64) at an early age.

- I learned the basics of computer programming early in life.

- I went to University of Kentucky for Computer Science.

- I got a Cooperative Education/Internship opportunity with a company (Department of Defense).

- I went to the University of California at Davis for Computer Security.

- I finally got an official penetration testing position.

- Even after a few different companies, I am still doing pentesting, now for TrustedSec.
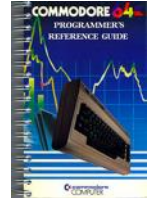
# How did Tyler get here?

- Started programming with a TI-99/4A at age 8.

- Learned programming from then through high school.

- Earned by Computer Science BS at U of Akron.

- Was a UNIX Sys Admin until I got my first info sec job.

- Worked around, did pen testing, fell in love with malware analysis and DFIR.

- Did a lot of online challenges/CTFs to increase my skills.

- Been doing IR ever since, and still love it!

# Your path may be VERY different than ours… and that is okay.

# Information Security Careers

# Information Security (InfoSec) Careers

- There is not just 1.

- 2 Basic Types
    - Attacker/Red Team
    - Defender/Blue Team

- Incident Response and Forensics
    - Malware Analysis

- But that is just the surface.
    - Red Team, Blue Team, Pentesting, Auditor, Developer, …

Picking your Path

# Common questions I get asked…

- How do I get to be a hacker?

- What are companies looking for in employees?

- How do I get a job that requires experience if I need a job to get experience?

- Do I need a college degree?

- How can I show people what I know, legally?

- What certifications do I need?

- Should I stay general or specialize?

- Do I need to know how to program?

- Do I need to learn <insert OS/hardware/topic/etc..>?

# What are companies looking for?

- Type 1 characteristics

  - Hard worker

  - Analytical

  - Self motivated

  - Problem solver

- Type 2 characteristics

  - Have experience

  - Knowledgeable

  - Well spoken/written

  - ***Certifications***

# Gaining Experience

# Gaining Experience

- **Take classes/College**

# Gaining Experience

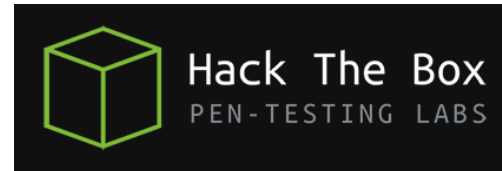- Take classes/College

- **Build a home lab**

# Gaining Experience

- Take classes/College

- Build a home lab

- **Participate in Capture the Flag (CTF)/Hack competitions**

# Gaining Experience

- Take classes/College

- Build a home lab

- Participate in Capture the Flag (CTF)/Hack competitions

- **HackTheBox and similar sites.**

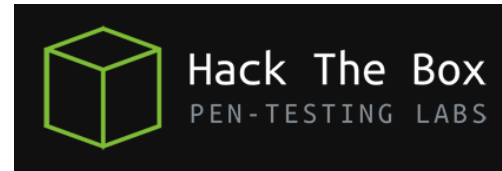# Gaining Experience

- Take classes/College

- Build a home lab

- Participate in Capture the Flag (CTF)/Hack competitions

- HacktheBox and similar sites.

- **Bug Bounties**

# Building Knowledge

# Building Knowledge

- Take classes/College

# Building Knowledge

- Take classes/College

- Attend security conferences

# Building Knowledge

- Take classes/College

- Attend security conferences

- Watch InfoSec videos

# Building Knowledge

- Take classes/College

- Attend security conferences

- Watch InfoSec videos

- **Read books**

# Building Knowledge



- Take classes/College

- Attend security conferences

- Watch InfoSec videos

- Read books

- **Meet people in the field and talk to them**

# Building Knowledge

- Take classes/College

- Attend security conferences

- Watch InfoSec videos

- Read books

- Meet people in the field and talk to them

- **Learn by doing**

# Presenting Yourself

# Presenting Yourself



- Start a blog

# Presenting Yourself

- Start a blog

- If you are a programmer, get of GitLab/GitHub and upload your code

# Presenting Yourself

- Start a blog

- If you are a programmer, get of GitLab/GitHub and upload your code

- Create videos

# Presenting Yourself



- Start a blog

- If you are a programmer, get of GitLab/GitHub and upload your code

- Create videos

- **Attend conferences**

  - **Present at conferences**

# Presenting Yourself

- Start a blog

- If you are a programmer, get of GitLab/GitHub and upload your code

- Create videos

- Attend conferences

  - Present at conferences

- ***Prepare a well written resume***

- ***Perform mock interviews***

# Certifications

- Are they required?

- Are they needed?

- Which ones should I get?

# More Questions…

- Should I stay general or specialize?

# More Questions…

- Should I stay general or specialize?

  - It depends

# More Questions…

- Should I stay general or specialize?

    - It depends

- **Do I need to know how to program?**

# More Questions…

- Should I stay general or specialize?

    - It depends


- Do I need to know how to program?

    - Yes/No...

    - Software Engineering degree not required

    - Ability to "script" (bash/python/powershell) very useful

# More Questions…

- Should I stay general or specialize?

  - It depends

- Do I need to know how to program?

  - Yes/No…

  - Software Engineering degree not required

  - Ability to "script" (bash/python/powershell) very useful

- **Do I need to learn <insert OS/hardware/topic/etc..>?**

# More Questions…

- Should I stay general or specialize?

  - It depends

- Do I need to know how to program?

  - Yes/No…

  - Software Engineering degree not required

  - Ability to "script" (bash/python/powershell) very useful

- Do I need to learn <insert OS/hardware/topic/etc..>?

  - **Maybe.**

  - **Depends on the company and the position**

In Closing…

# Final Thoughts

- You decide your future.

- There is not 1 InfoSec job for everyone.

- Everyone has their own experiences and talents.

- Find what you enjoy and are good at.

- Always keep learning and expanding your knowledge base.

The information security industry is constantly evolving—keep up by following TrustedSec's active social media, blogs, podcasts, and webinars.

# TRUSTEDSEC.COM

With a goal of always doing the right thing for our clients and the industry, TrustedSec conducts research, develops new tools, administers training classes, and keynotes, presents, and hosts security conferences throughout the world.
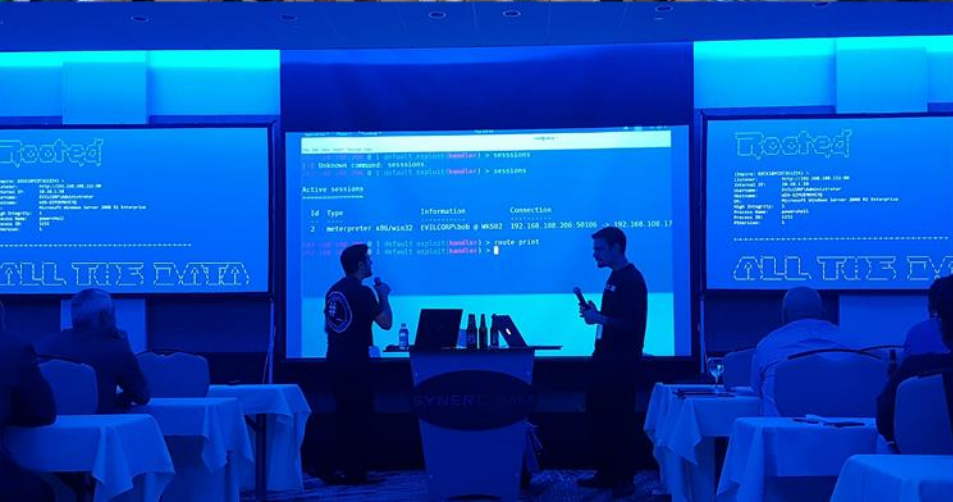
# Questions?

**TRUSTEDSEC**

TRUSTEDSEC.com 🐦 @TRUSTEDSEC