Continuous

Improvement

For Everyone

- Matt Scheurer


@c3rkah | 
https://www.linkedin.com/in/mattscheurer/


https://www.slideshare.net/cerkah/

About Me

I work here:

first financial bank

FDIC

As a Sr.
Systems Security Engineer

I serve as Chair for the

CiNPA
Cincinnati Networking Professionals Association
Security Special Interest Group

43 69 6e 63 69 6e 6e 61 74 69 20 4e 65 74 77
6f 72 6b 69 6e 67 20 50 72 6f 66 65 73 73 69
6f 6e 61 6c 73 20 41 73 73 6f 63 69 61 74 69
6f 6e 20 53 65 63 75 72 69 74 79 20 53 70 65
63 69 61 6c 20 49 6e 74 65 72 65 73 74 20 47
72 6f 75 70 3a 20 63 69 6e 70 61 2e 6f 72 67

SECURITY SIG

I am also an
Ambassador & Security Researcher for

bugcrowd

Objectives

- Provide attendees with ideas and options for continuing to expand their Information Security skills
  - Not all of these ideas will appeal to everyone
    - Pick and choose the right ones specifically for you
  - Examples provided are not exhaustive lists
    - There are considerably more resources than I can cover
    - If there is something missing, please let ~~me~~ **us** know!

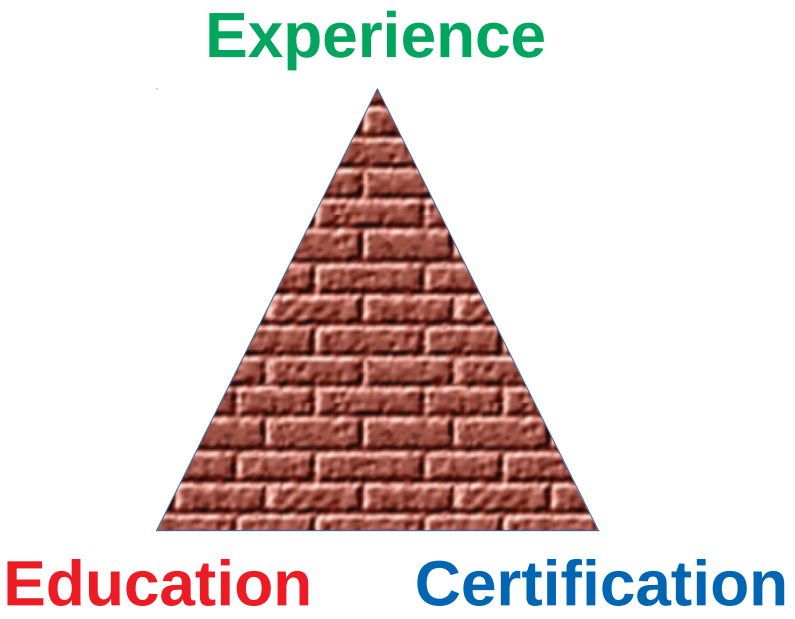
Why (should I do any of this)?

- Developing and improving your skills helps whether...
  - You are looking for that first career opportunity
  - Looking to take that next career step
  - Making impacts to safeguard your own job security
  - You want to help mentor others
  - You are looking for ways to give back / get involved

Inspirations for this Talk

- Creative workarounds to learning with
  - Very limited time
  - Zero training budget
- Free educational sites
- Other conference speakers & talks
- Articles, Blogs, Podcasts, & Videos
- Bugcrowd University
- Personal Experience
  - Running a monthly local InfoSec meetup group
  - Mentoring others

The Qualification Triangle



- Experience is typically the most valued by employers
- Triangle doesn’t account for
  - Luck
  - Security Clearance
  - Emotional Intelligence Quotient (EIQ)

InfoSec Street Cred?

- Getting that first opportunity in InfoSec is hard!
  - Some get lucky with a good co-op or internship
- Equipped with only a degree(s) and/or certifications alone, the world will probably not beat a path to your door in spite of the number of open positions in InfoSec and skills gaps
  - But I do have some ideas!

Standing out from the Crowd

- Ideas to demonstrate passion and knowledge
  - Writing
  - Recording and posting new Tech Videos
  - Volunteering
  - Bug Bounties
  - Teaching Others

Writing Examples

- Tech Articles
- Tech Blogs
- White Papers

- Event Write-Ups, such as:
  - Key Takeaways
  - Lessons Learned

Video Lesson Examples

- **Record & Post Videos**

- YouTube Channel? (Maybe Not Right Now)

  - BitChute or other YouTube alternatives

Volunteering Examples

- Technology Conferences
- Information Security / Hacker Conferences

- Local Tech & InfoSec Meetup Groups
  - Most groups want help, even if it’s not publicized

Teaching Others at...

- Conferences
- Meetup Groups
- Webinars
- Workshops
- Brown Bag Lunches
- School Labs
- Library Rooms
- Hallways
- Everywhere Else!

Learning & **Teaching** Opportunities

CYBRARY

PLURALSIGHT

Bug Bounty Programs

- Get Paid to Hack Stuff!
  - Legally and Ethically!!!
  - Also gain professional experience

- And / Or -

- Consider Entering CTF Competitions
  - Add personal skills and increase proficiency

Tying it all Together

- Publicly journal the things you learn when you
  - Take a class, participate in a CTF, attend a workshop, earn a certification, complete an online challenge or course, conduct research, etc.?
  - Publish a write-up, or post a video recap, or both
  - Present at local meetup groups & conferences
- Put these activities on your Resume!

Learning

- There are plenty of ways to learn new things
  - And probably more places now than ever before
  - But I still learn best through hands-on activities and time in the seat
- Let’s look at some free and low cost examples...

SEED labs

The SEED project's objective is to develop hands-on laboratory exercises (called SEED labs) for computer and information security education and help instructors adopt these labs in their curricula. At present, there are over 30 labs available.

Web site:

https://seedsecuritylabs.org/

SEED labs - Software Security

- Buffer Overflow Vulnerability Lab
- Return-to-Libc Attack Lab
- Environment Variable and Set-UID Lab
- Race Condition Vulnerability Lab
- Dirty COW Attack Lab
- Format String Vulnerability Lab
- Shellshock Vulnerability Lab

SEED labs - Network Security

- Packet Sniffing and Spoofing Lab
- TCP/IP Attack Lab
- Heartbleed Attack Lab
- Local DNS Attack Lab
- Remote DNS Attack Lab
- Firewall Exploration Lab
- Firewall Evasion Lab
- Virtual Private Network (VPN) Lab

SEED labs – More Attack Labs

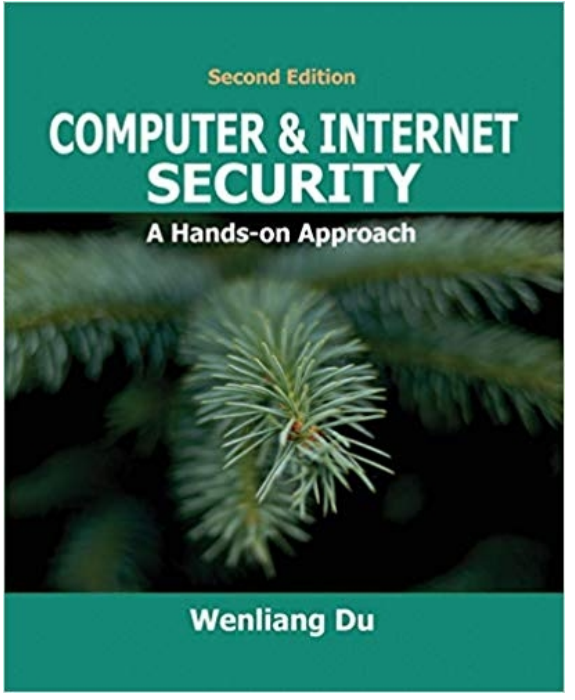
- Web Security Labs
  - Cross-site Scripting Attack Lab
  - Cross-Site Request Forgery Attack Lab
  - SQL Injection Attack Lab
- System Security Labs
  - Meltdown Attack Lab
  - Spectre Attack Lab

SEED labs – Still More Labs

- Cryptography Labs
  - MD5 Collision Attack Lab
  - RSA Public-Key Encryption and Signature Lab
  - Secret Key Encryption Lab
  - Pseudo Random Number Generation Lab
  - Public-Key Infrastructure (PKI) Lab
- Mobile Security Labs
  - Android Repackaging Attack Lab
  - Android Device Rooting Lab

SEED labs Caveats

The online documentation is sparse. You will want to order Dr. Wenliang (Kevin) Du's accompanying "Computer & Internet Security: A Hands-on Approach" Second Edition book (~$70) to get the most out of these open labs.



ENISA Training Labs

Created by the European Union Agency for Cybersecurity (ENISA), the ENISA CSIRT training material, containing Handbooks for teachers, Toolsets for students and Virtual Images to support hands on training sessions.

Web site:

https://bit.ly/296L1Ae

ENISA Labs – Technical (1/2)

- Building artifact handling and analysis environment
- Processing and storing artifacts
- Artifact analysis fundamentals
- Advanced artifact handling
- Introduction to advanced artifact analysis
- Dynamic analysis of artifacts
- Static analysis of artifacts
- Forensic analysis: Local Incident Response
- Forensic analysis: Network Incident Response
- Forensic analysis: Web server Analysis
- Developing Countermeasures
- Common framework for artifact analysis activities

ENISA Labs – Technical (2/2)

- Using indicators to enhance defence capabilities
- Identification and handling of electronic evidence
- Digital forensics
- Mobile threats incident handling
- Mobile threats incident handling (Part II)
- Proactive incident detection
- Automation in incident handling
- Introduction to network forensics (New)
- Honeypots
- Vulnerability handling
- Presenting, correlating and filtering various feeds

ENISA Training Labs Caveats

These labs are built with a noticeable international focus as created by the EU. GMT lab times are different from USA time zones. Documentation is written in International English not US English. Legal references are not always applicable in the United States.

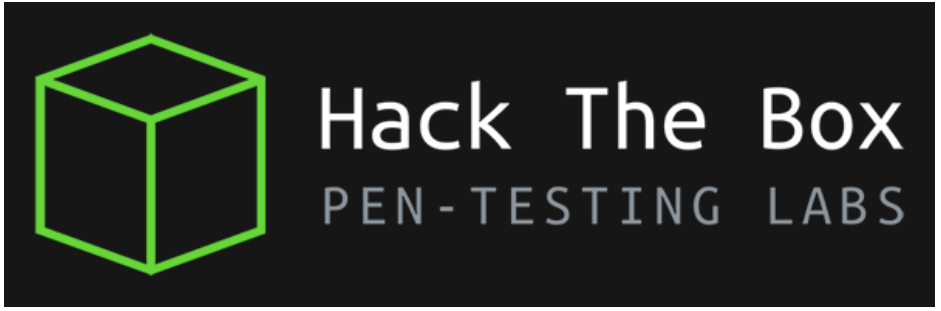
Bugcrowd University

Bugcrowd University is a free and open source project for security, education, and training for the whitehat hacker community. Learn the basics of hacking and bug bounty hunting with videos, tutorials, labs, best practices and more.

Web site:

https://bit.ly/2NAit8r

More Free Hands-On Learning



Hack Yourself First:
How to go on the
Cyber-Offense

AppSec Hands-On Learning

OWASP

Open Web Application Security Project

Mutillidae 2

Goal Setting

- If you could do anything you would like in the next 5 years, what would it be?
- List out the steps along the way you think a person would take in order to get there
- Do those things in your action plan

Jim Cathcart Quotes

“Think Like the Person You Intend to Become.”

“If You Will Spend One Extra Hour Each Day Studying Your Chosen Field, You’ll Be a National Expert in That Field in Five Years or Less.”

Emotional Intelligence

Emotional intelligence (EI), emotional leadership (EL), emotional quotient (EQ) and emotional intelligence quotient (EIQ), is the capability of individuals to recognize their own emotions and those of others, discern between different feelings and label them appropriately, use emotional information to guide thinking and behavior, and manage and/or adjust emotions to adapt to environments or achieve one's goal(s).

https://en.wikipedia.org/wiki/Emotional_intelligence

Building up those Soft Skills

It may sound too touchy-feely for some at first, but I honestly attribute EIQ for reaching my professional goals. Many studies conclude that people with the highest EIQ typically achieve more success and higher compensation than even the smartest people.

There are lots of great articles through the following Google search:

improving “emotional intelligence”

I recommend bookmarking the one’s most beneficial to you and revisiting them occasionally as refreshers.

Mom quotes before EIQ was a thing

- *“It’s not always what you know, but sometimes who you know.”*
- *“Always treat others as you would like to be treated.”*
- *“If you don’t have anything nice to say then you shouldn’t say anything at all.”*
- *“Nobody cares how much you know until they know how much you care.”*

My Advice...

Leave the “Trolling” and flame wars to Orville!

Conclusions

- Experiment and find what works best for you

Conclusions

- Experiment and find what works best for you
- Market yourself well (You’re in charge of your own personal brand)

Conclusions

- Experiment and find what works best for you
- Market yourself well (You’re in charge of your own personal brand)
- Work hard and share these lessons with others

Conclusions

- Experiment and find what works best for you
- Market yourself well (You’re in charge of your own personal brand)
- Work hard and share these lessons with others
- Never stop learning or challenging yourself

Conclusions

- Experiment and find what works best for you
- Market yourself well (You’re in charge of your own personal brand)
- Work hard and share these lessons with others
- Never stop learning or challenging yourself
- Don’t forget those Soft Skills (i.e., EIQ)!

Questions

Who ...

What ...

When ...

Where ...

Why ...

How ...

Continuous

Improvement

For Everyone

Thank you for attending!

@c3rkah | https://www.linkedin.com/in/mattscheurer/

https://www.slideshare.net/cerkah/