BISHOP FOX®

Lessons on Security Consulting

WHAT I'VE LEARNED SINCE GRADUATION

TechTrek
UAT Discovery Expo

November 06, 2014

About Me

ZACH JULIAN

Lives – In Tempe, AZ

Works – At Bishop Fox, a global security consulting firm

Graduated – From UAT in 2012 with degree in Network Security

First, let's discuss some of the common roles within the information security industry.

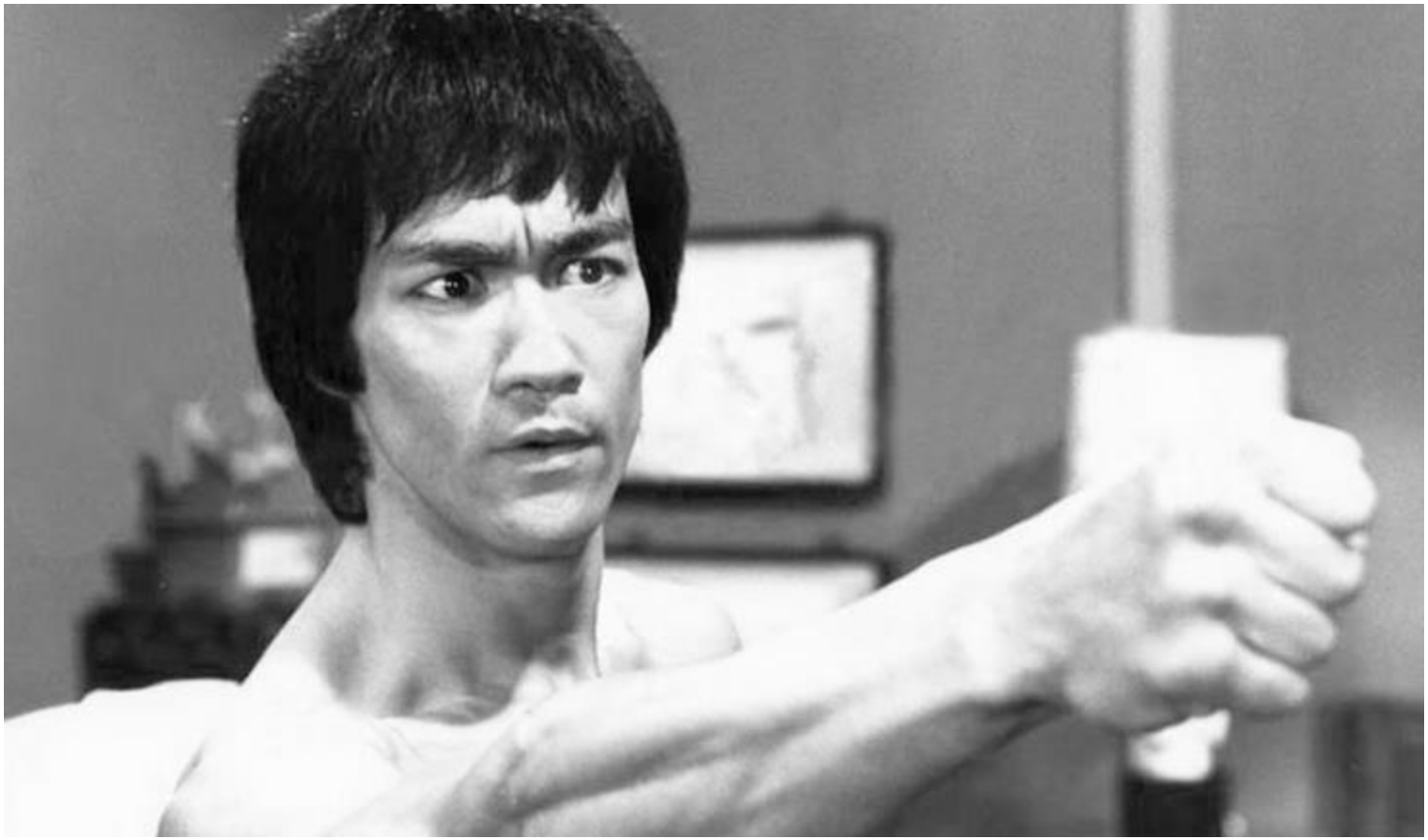
The ‘Security Industry’ is Big

...AND HIGHLY SPECIALIZED

- Information Security is made of many specialized roles
- Some examples:
  - Web Application Pentesting
  - Networking Pentesting
  - Malware Analysis / Reverse Engineering
  - Network Engineering
  - Security Architecture
  - Network-level controls
  - Cryptography
  - Compliance
- Take advantage of time in school to find your niche and work on projects that interest you

Focus!

HARNESS YOUR INNER NERD



Choices After Graduation

WHEN ITS TIME TO BRING HOME THE BACON

- In-house
- Freelancing
- Teaching
- Consulting

CONSULTING

BECOMING A TRUSTED ADVISOR

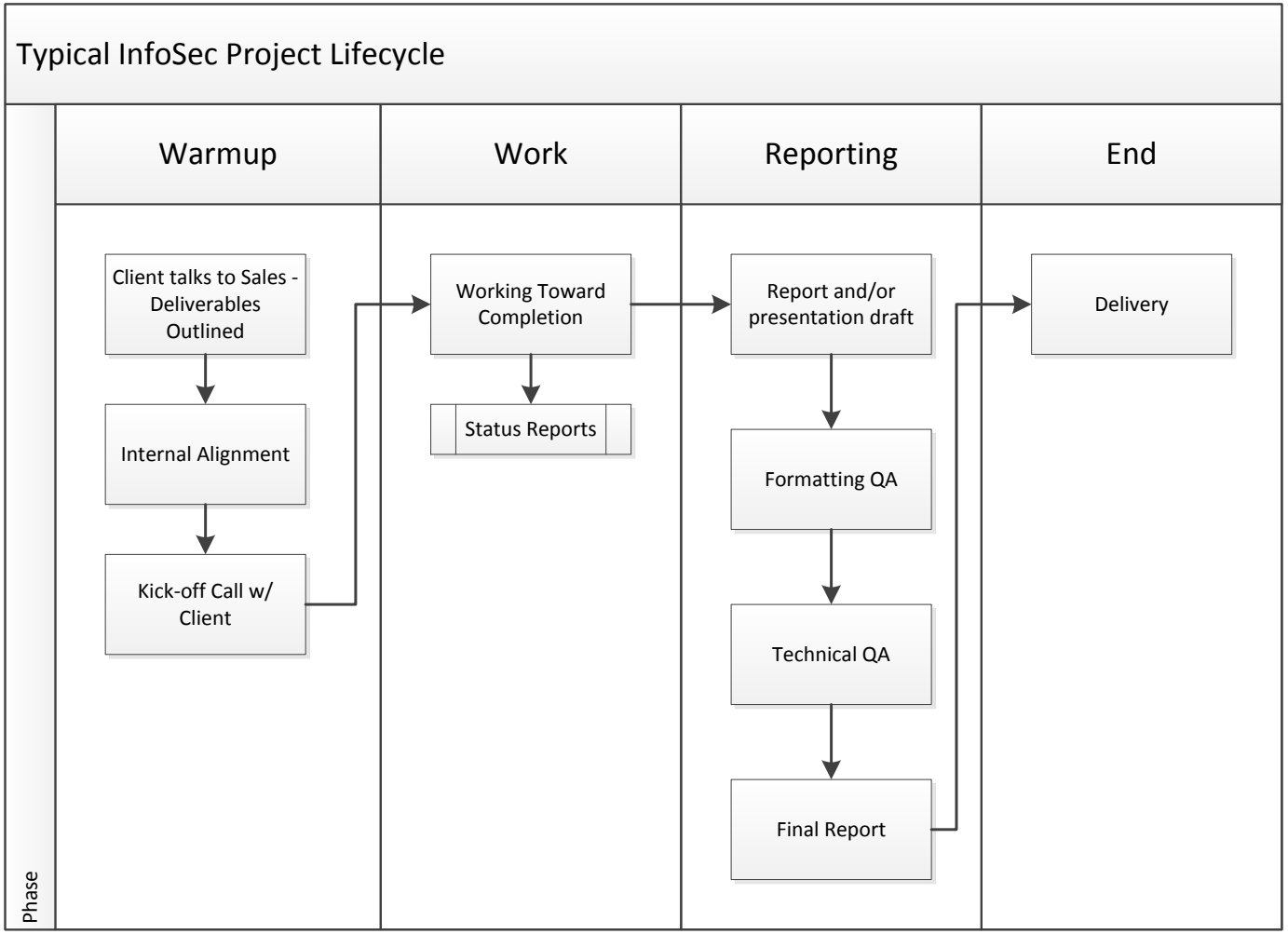
What is Consulting?

AND WHY DO COMPANIES NEED IT?

- Our customers: companies who need help meeting a technical challenge
- Security consulting covers a wide range of business needs
- Clients are looking for a trusted advisor

What Does a Project Look Like?

TYPICAL PROJECT LIFECYCLE



What are some of the main differences between working at a consultancy and working in-house?

Consulting vs. In-House: Positives

WHAT'S THE DIFFERENCE?

- Traveling
- Wide variety of projects and technologies to learn
- Flexible working hours and location
- Small company culture
- People listen to your recommendations
- You can affect changes on household companies

Good consultants are able to adapt quickly to new technologies.

Consulting vs. In-House: Challenges

WHAT'S THE DIFFERENCE?

- Multiple 'bosses'
- Balancing projects - scheduling is key
- Improved soft skills are required
- Potentially longer hours

TECHNICAL SKILLS

BECOMING A TRUSTED ADVISOR

Web Application Security: Concepts

CONSIDER THE FOLLOWING

- Learn the OWASP Top 10
- Familiarize yourself with SQL
- Learn the ins and outs of common protocols – TCP/IP, HTTP, DNS
- Understand ways of encoding & transporting data

Web Application Security: Tools

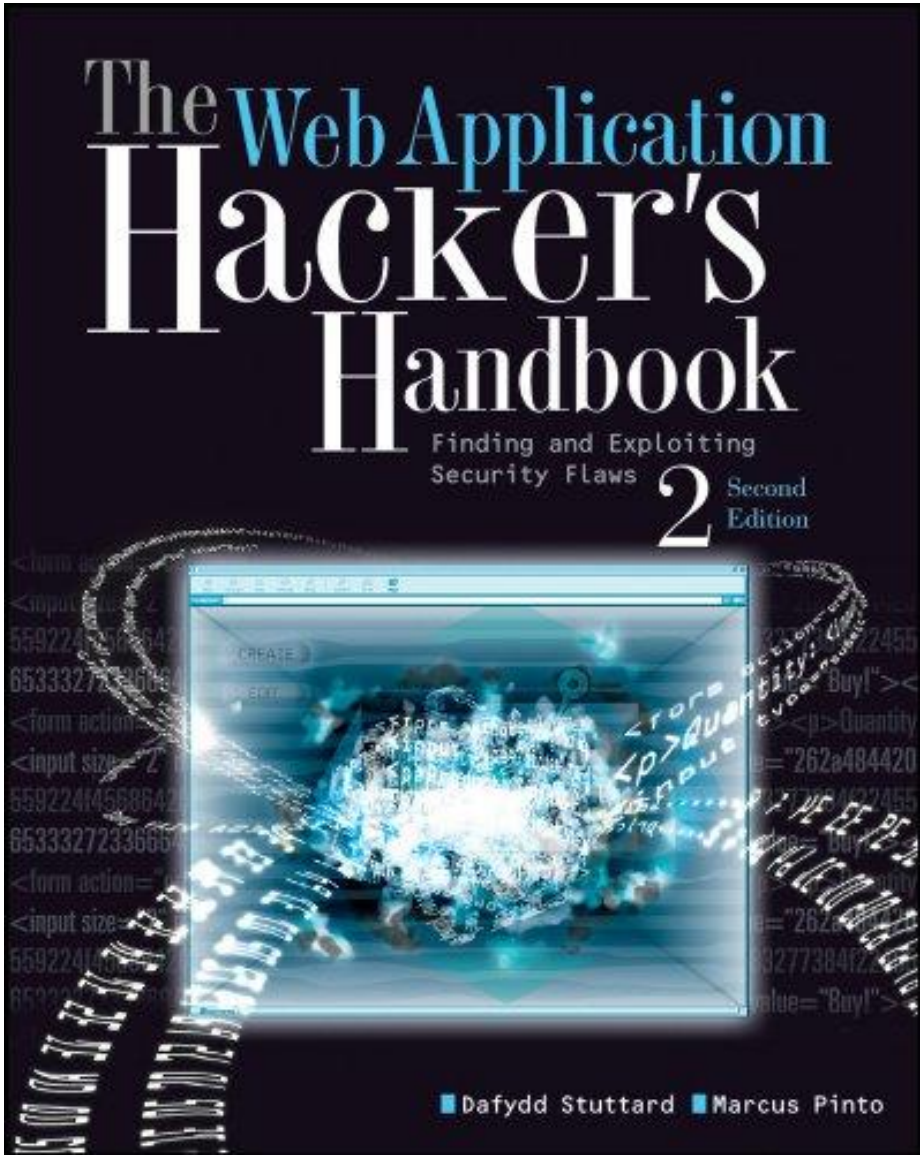
YOUR ARSENAL

- Master Burp Suite Pro
- Learn how to use Metasploit
- Learn the Linux command line & Bash scripting
- Pick up a language like Python
- Try out a vulnerability scanner

More Security Tools

YOUR ARSENAL

- netcat
- nmap
- dirbuster/nikto
- sqlmap
- BeEF
- Meterpreter
- Maltego
- SearchDiggity


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard
Marcus Pinto

Network Engineering: Concepts

CONSIDER THE FOLLOWING

- Become comfortable with network diagrams
- Windows & UNIX networking concepts
- Install & configure common services:
  - SSH, mail, HTTP, IRC

Network Engineering: Tools

CONSIDER THE FOLLOWING

- Learn tcpdump arguments
- Experiment with an IDS: SecurityOnion
- Write some IDS rules
- Explore Splunk

Security Auditing: Concepts

CONSIDER THE FOLLOWING

- Compliance standards:
  - PCI
  - NERC CIP
  - SOX
  - HIPAA
- Regular Expression & Bash scripting

Security Architecture: Concepts

CONSIDER THE FOLLOWING

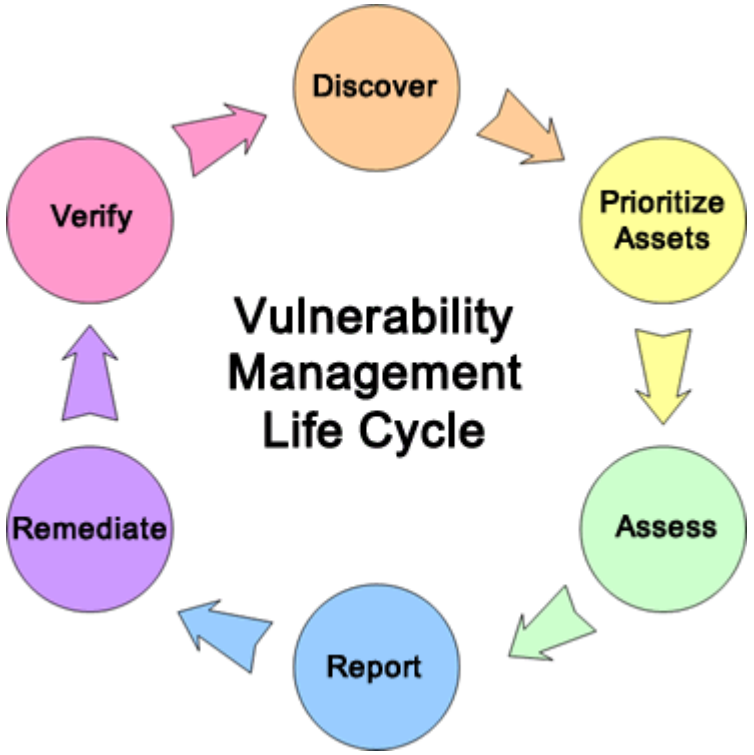
- It is common for clients to need help with a security process
- Vulnerability Management
  - Patch Management
- Log Management
- Access Management
- Incident Response

- “We have X tool and need it to work with Y process”

Security Architecture: Concepts

CONSIDER THE FOLLOWING

- One issue can be indicative of others
- Learn how companies usually handle common processes:
  - NIST Special Publications
  - SANS Whitepapers
  - Others



SOFT SKILLS

BECOMING A TRUSTED ADVISOR

Writing

SOUND LIKE YOU KNOW WHAT YOU'RE TALKING ABOUT

- Professional writing skills are key
- Avoid endless QA cycles
- A well-written email can defuse many situations
- Documentation

Listening to Clients

WHAT DOES THE CUSTOMER WANT?

- What goal is the client trying to fulfill?
- “What encouraged this activity?”
- Pro-tip: Always take notes

Communicating to Executives

EXPLAINING TECHNICAL CONCEPTS TO NON-TECHNICAL PEOPLE

- Most projects involve an executive deliverable
- Avoid being condescending
- Not negatives, but opportunities

Corporate Politics

DIFFICULT SEAS TO NAVIGATE

- Consultants must be cautious of customer's internal politics

- Listen carefully to customer requests

Other

VARIOUS SOFT SKILLS

- Have business attire at the ready
- Be cognizant of your appearance

CAREER BUILDERS

EXTRACURRICULAR ACTIVITIES

The best hackers treat InfoSec as a lifestyle rather than a career.

Never Stop Creating

PUT YOURSELF AND YOUR WORK OUT THERE

- Github is the new résumé
- Never stop researching your area of interest
- Blog about your solutions to tough problems

Promote Yourself (at Conferences & Events)

PUT YOURSELF AND YOUR WORK OUT THERE

- Discover something? Make a tool? Have an idea?

  Give a talk about it

- Start with local events to gain confidence

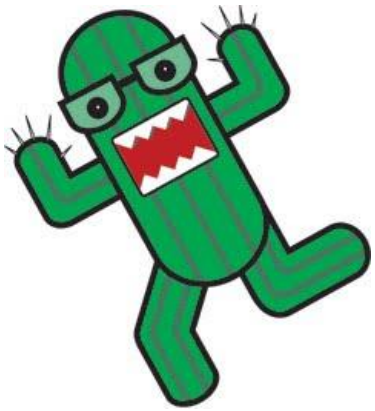
- Establish an online presence – Twitter is popular among security professionals

- Organize events!

Phoenix IT/Security Events & Meetings

A LIST TO GET YOU STARTED

- Heat Sync Labs
- PHX2600 monthly meetings
- CactusCon
- Southwest Security Professionals Forum
- Desert Code Camp
- CryptoParty PHX
- ISACA Phoenix



Outside Phoenix:

- ToorCon
- BlackHat / DEF CON
- WRCCDC (Blue Team/Red Team)

Thank You

TechTrek
UAT Discovery Expo

BISHOP FOX®