Royal Team Testing

Purple Teaming to Build and Secure Applications

Kevin Johnson
CEO
Secure Ideas, LLC
904-403-8024
kevin@secureideas.com
@secureideas

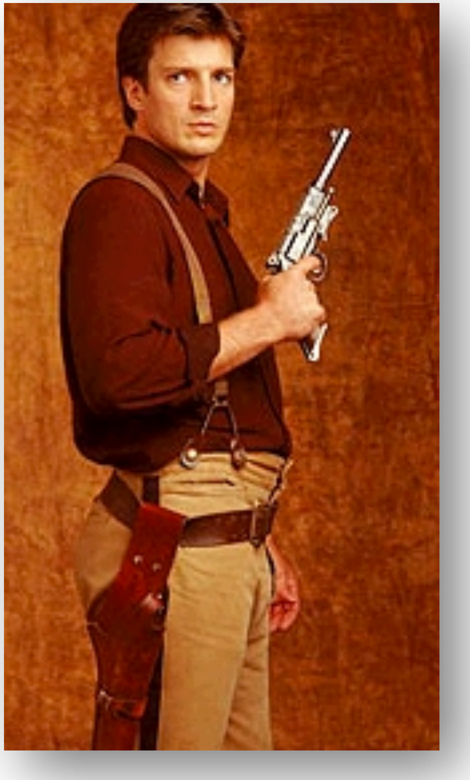
SecureIdeas
professionally evil

Kevin Johnson

- Founder and CEO of Secure Ideas
- IANS Faculty Member
- Course Author and Instructor
  - Web Application and Mobile Testing
  - BlackHat, DerbyCon, OWASP
- Podcaster
  - Professionally Evil Perspective
- Open Source Project Lead
  - SamuraiWTF, Laudanum, Yokoso, WeaponizedFlash, etc.
- 501st Member - TI-42265
- Father, Husband and Christian

Wild West?

- Security is a big topic today
  - I don't think I needed to say that! ;)
- Risks, vulnerabilities and threats
  - And everything related to them
- Tons of issues exist
  - Hackers, hacktivists, disgruntled users and mistakes
  - New technology, legacy support and business requirements
- Our jobs are more difficult today
  - And maybe more fun?



Protecting Ourselves

- How do we know the threats?
  - And where do they come from?
- Understanding vulnerabilities
  - Discovering them?
- Do we test
  - Required to test?
- What do we control?
  - Cloud? Devices? Software?

Development & Purchasing is Accelerating

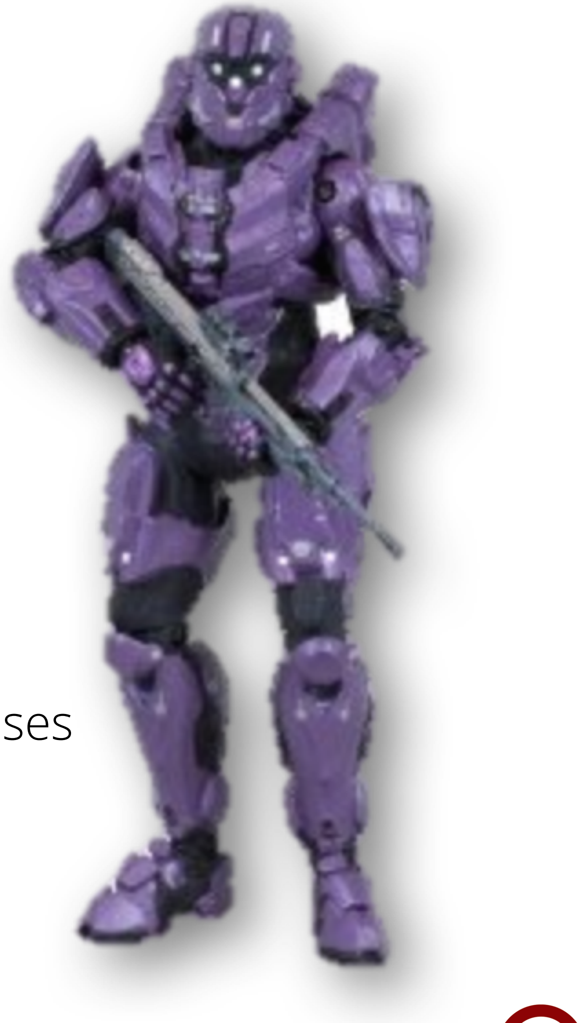
- Businesses have embraced technology
  - Its everywhere ;)
- Applications have become a main focus
  - Everyone wants to be a developer
- Even purchasing has gotten in on the mix

Agile Development

- No more semi annual releases
  - Releases happen weekly or even daily
- Development done in short sprints
  - Less time for traditional security testing
- This is another main topic today

Combine Red and Blue

- Separating attack and defense causes issues
  - Less comprehensive
  - Missing the understanding of the attack
- Organizations often treat these are completely different functions
  - SOC versus Testing versus users
- Combining the two sides also has benefits
  - Better understanding of risk
  - Clearer view of the issues and vulnerabilities
- Better understanding of risk
  - We need to be aware of what the risk is
  - Understanding the attacks and the controls/defenses
- Clearer view of the issues and vulnerabilities
  - Defense understands the systems and controls
  - Offense understands the adversary



What Do We Look For

- We need to find the flaws
  - Without exploiting them greatly
- Common OWASP issues are a start
  - Top 10, but more
- Don't forget logic and process attacks
  - Harder to find but bigger impact

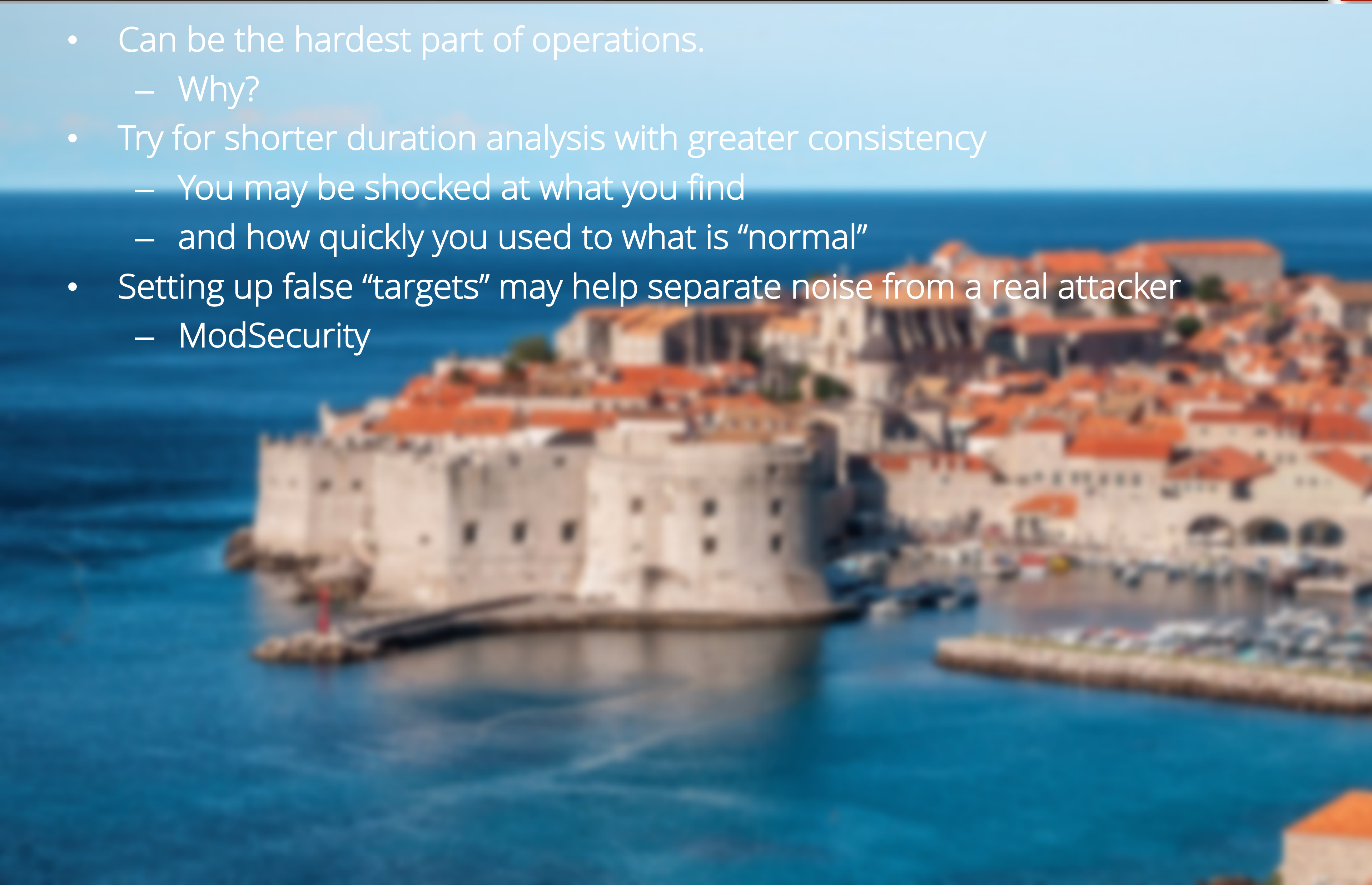
Understanding Attacks

- Understanding various attacks helps with security
  - How can you prevent something without understanding it
- This is a core foundation of penetration testing
  - Know the vulnerabilities and exploits possible
- This understanding requires us to know the attacks possible
  - And how to find the flaws they target

Understanding Context

- Context is probably the most critical skill
  - Context is a major foundation of our testing
- Context takes many forms
  - We have the application's context
  - The vulnerabilities and our attacks are a second context
- We have to understand the various contexts during our testing
  - Application Context
  - Vulnerability Context
  - Exploit Context

What about Blue?



- Can be the hardest part of operations.
  - Why?
- Try for shorter duration analysis with greater consistency
  - You may be shocked at what you find
  - and how quickly you used to what is “normal”
- Setting up false “targets” may help separate noise from a real attacker
  - ModSecurity

Understand Logging

- Review your logs
  - What does the application record?
- Look for signs of attack
  - Based on the testing?
- All logging is in scope
  - System
  - Application
  - Infrastructure

Purple?

- Combine the two sides
  - During pentesting
- Work with your testers
  - Ride-along?
- Mimic analysis during an incident
  - Better than table top
- Guide the testing
  - Based on developer knowledge of the application

Royal Team Testing

Purple Teaming to Build and Secure Applications

Kevin Johnson
CEO
Secure Ideas, LLC
904-403-8024
kevin@secureideas.com
@secureideas

Secure Ideas
professionally evil℠