# Training the Next Generation of Penetration Testers (NG PT)

**Kostas Papachristofis (MSc, MBA)**
InterLei, Educational ICT Consultant/Instructor
Security Expert (CCNP Sec)

# Get you hands dirty

(Take the view of the attacker to see if your defenses are working)

## CURRENT APPROACH

VERSUS

## NG APPROACH

**General Theory & Methodology**

**Unstructured Information**

**Certifications (theory)**

**General Tools**

**Results/outcomes interpretation difficulties**

**How to defend yourself**

**Technical skills (theory and labs)**

**Structured Information**

**Certifications (theory and labs)**

**Tools  needed to achieve a specific attack (Hands-on)**

**Interpretations of the results. Next Steps**

**Both how to attack and defend**

**Mitigation Techniques – Secure your environment**

# Common defense measures

1. Firewalls
2. VPN & Private networking
3. Intrusion Prevention Systems
4. Domain Controller (Group Policy)
5. Anti-virus/Anti-spam/Content filtering
6. Off-site Backups

# But these defense measures didn’t work…

1. YAHOO data breach
2. USA Presidential Election hacks
3. SWIFT hack
4. LinkedIn data breach
5. Adult Friend Finder data breach
6. Database of Philippine election voters hacked

# Trust the Best Penetration Experts

| interLei | encode | TWELVE SEC |
|---|---|---|
| 600+ Companies & 5000+ Students | 200+ Companies & 1300+ Projects | 150+ Companies & 250+ Projects |
| 7+ Cisco, Microsoft, Oracle LPI, RedHat, ITIL VMware | 16 Years in Cyber Security; 250+ APT Simulations | 250+ projects Penetration Tests, Vulnerability Assessments and Red/Purple Teaming Exercises |
| 22 6 CCIE, 7 CCNP R/S/C/DC/W, 5 MCT, 1 Oracle OCM, 1 LPI L3, 2 RH | 80 Certified Engineers, Sales and Presales | 26 team certifications C\|EH, OSCP, CISA, CISM, CISSP, CISSP- ISSAP, CRISC, ISO 9k A/LA, ISO27k LA/A, IT/IL v3(F), SOTP, CSSLP, CCNA, RHCSA |
| AWARDS Cisco Excellence Award 2014/2015 1st Oracle Partner (Workforce Dev. Prog) | AWARDS Top #29 in Europe by CyberSecurityVentures IBM Beacon Award – Outstanding Security Solution | 6 sectors European Commission, Financial Institutions, Law Enforcement, Health, Governments, International Agencies |

# Network and System Penetration Testing (40H Training and Challenge)

- Passive Information Gathering
- Active Information Gathering
- OSINT - Target Profiling

- Social Engineering
- Targets Enumeration
- Vulnerability Analysis

- Exploit Development and Finetuning
- Exploitation
- Post Exploitation

- Access Persistence
- Covert Operations
- Red/Purple Teaming
- Reporting

- Wi-Fi Assessment
- SCADA/ OT Assessment
- IoT Assessment
- Physical Security Bypass

**THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY ENGINEER**

interLei

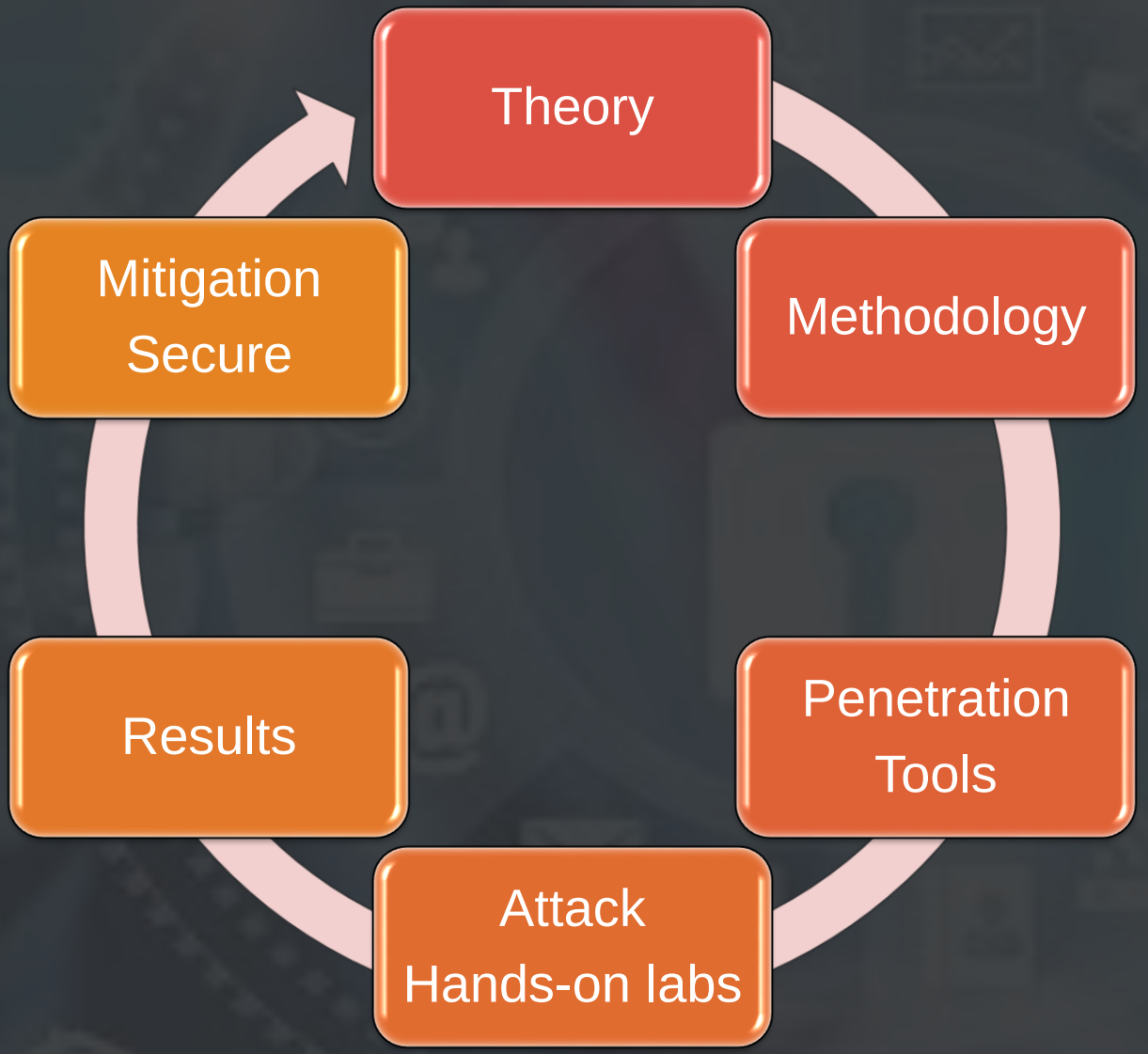
# Web Application Penetration Testing (16H Training and Challenge)

- Application Mapping
- Technology Related Attacks
- OWASP Testing Guide - Hands On
- Business Logic Vulnerabilities
- Horizontal/Vertical Escalation
- Using a web proxy
- Application specific scripting
- Reporting

**LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK**

interLei

# Training Courses - Benefits



# Reasons to follow the trainings…

1. Ideal for Ethical hackers, Penetration Testers, IT Engineers, Web developers, Security personnel, Defenders, Auditors, Forensics specialists
2. Increase your security skills, improve CV and salary, new job opportunities
3. Expose weaknesses in your organization
4. Test and improve your security
5. Become the NG Penetration Tester. Create your own success story
6. Talk to instructor – Learn the security secrets from the experts- Not self-paced
7. Prepare for OSCP, CEH
8. Certificate of Attendance (Challenge)

# THINK LIKE A HACKER

# THANK YOU

## WANT TO KNOW MORE ?


We will be happy to meet you on **Interlei's** booth