



INTRODUCTION

Introduction to Penetration Testing

AMIN HAMID / RUFIO

- Co-Founder of StrykeLabs.
- Currently working for a fortune 50 company in the field of Global Security Incident Response.
- Hack in The Box core crew member since 2006.
 - CTF Overlord from 2008 – 2011.
- Over 10 years of hands on offensive security experience.
- 5 years of penetration testing in APAC and Europe.
- Research interests in the areas of embedded devices and web hacking.
- Presented at HITB2011KUL & HITR2NDB (Utrecht) 2011.

EARL MARCUS / KLKS

- Over 10 years of hands on offensive security experience.
- 5 years of penetration testing and RedTeam activities for a fortune 50 company.
- Hack in The Box core crew member since 2010.
 - CTF crew member.
- Primary passion is in the field of reverse engineering and malware analysis.
- Works on electronic projects, and occasional exploit writing.

COURSE OUTLINE – DAY 1

9.00 am // Introduction to IT security

- Basic requirements of IT security
- Different types of threats
- IT security measures

10.00 am // Introduction to penetration testing

- What is a penetration test
- Classification of different tests
- Devising penetration tests
- Limits of penetration testing

10.30 am // Morning tea break

COURSE OUTLINE – DAY 1

11.00 am // Preparations

- Organisational requirements
- Personnel requirements
- Technical requirements
- Legal issues
- Ethical issues
- Standards & guidelines

11.30 am // Attack vectors

12.30 pm // Lunch

COURSE OUTLINE – DAY 1

1.30 pm // Lab 1 – Penetration testing methodology

- Methodology
- Preparation
- Test procedures
- Tool selection

3.40 pm // Evening tea break

4.00pm // Lab 2 – Information gathering

- Reconnaissance
- Network mapping

COURSE OUTLINE – DAY 2

9.00 am // Lab 3 – Exploitation

- Vulnerability identification
- Vulnerability verification
- Exploitation

10.30 am // Morning tea break

COURSE OUTLINE – DAY 2

11.00 am // Lab 4 – Post exploitation

- Post exploitation activities
- Attacking internal targets maintaining access
- Clean up

12.30 pm // Lunch

1.30 pm // Lab 4 – Post exploitation (cont.)

COURSE OUTLINE – DAY 2

3.30 pm // Evening tea break

4.00 pm // Lab 5 – Documentation

- Final analysis of findings
- Reporting