## Week 6

Help

# Penetration Testing

Last week we looked at how automated tools could be used to assist developers and testers in finding important security bugs. We focused in particular on *static analysis* and *symbolic execution* as technologies.

This week, we will look at the broader practice of *penetration testing* of which tools using these technologies form some part, but other practices and techniques are of interest too. We will focus in particular on *fuzz testing*, a technique that attempts to find potentially security-relevant software failures.

## Learning Objectives

After the completion of this week's material, you will:

- Understand what penetration testing is and what it achieves
- Know the basics of several state-of-the-art penetration testing tools
- Understand fuzz testing techniques and how they compare
- Be aware of several state-of-the-art fuzz testing tools

## Video Lectures

- Penetration Testing: Introduction (10:11)
- Penetration Testing: Techniques and Tools (14:28)

- Fuzz Testing: Techniques and Tools (15:13)

## Break out: Interview with Eric Eames

In September 2014, Mike also interviewed Eric Eames, a Principal Security Consultant at FusionX. In this interview we discussed principles and practice of penetration testing. **The interview is *required*** from an assessment perspective -- some quiz material will be drawn from this interview's content.

Mike Hicks interviews Eric Eames (31:46). Highlights, indexed by time:

- start - Introduction and background
- 1:33 - Penetration testing: what is it?
- 5:04 - Tools and techniques used in penetration testing
- 9:43 - Common technical and human mistakes in engagements
- 15:05 - Defining an engagement; pen testers as outsiders or insiders
- 17:50 - Surprising discoveries
- 19:33 - What else, in addition to penetration testing can help ensure security
- 23:05 - Undergrad education -- what should we do?
- 26:39 - Prognosis for security, looking ahead

## Break out: Interview with Patrice Godefroid

In September 2014, Mike had the pleasure of interviewing Patrice Godefroid, who is a Principal Research at Microsoft Research. In this interview we discussed principles and practice of fuzz testing in general, and whitebox fuzz testing in particular, especially as it has come to be used within Microsoft. The interview is *optional* from an assessment perspective, but *recommended* -- there will no quiz questions on it per se, but it might help provide context about material from last week and this week..

Mike Hicks interviews Patrice Godefroid (35:06). Highlights, indexed by time:

- start - Introduction and background
- 1:08 - The state of the art in automated vulnerability detection
- 5:50 - What drove your interest in working on model checking/analysis?
- 10:13 - Comparing different fuzz testing techniques
- 19:21 - The story of deployment of fuzzing at Microsoft for whitebox fuzzing

- 24:57 - Trends in the use of automated analysis tools
- 31:06 - Open problems in automated testing tool development

---

# Supplemental Links

Here we present links to supplemental material, in case you are interested to read it (none is required for assessment).

- Ware report - introduced the idea of penetration testing, as well as many other foundational ideas in systems security
- CPT (pen testing) certification - establish your credentials as a pen tester
- Defcon CTF contest - be the first to find vulnerabilities in other competitors' systems and patch them in your own

## Penetration testing tools

These tools are all free, or have free versions.

- NMAP - "network mapper" scans network to find what's connected to it
- Zap - web proxy and automatic vulnerability scanner
- Burp suite - Several pen testing tools (some versions are free)
- Metasploit - customizable platform for developing, testing, and using exploit code.
- Kali - Linux distribution with pre-installed pen testing tools.

## Fuzz testing tools

Again, these tools are all free, or have free versions.

- Radamsa - mutation-based black-box fuzzer
- Blab - grammar-based fuzzer
- American Fuzzy Lop - mutation-based, white-box fuzzer
- CERT basic fuzzing framework (Zzuf) - found many high-profile bugs
- Sulley - lots of extras to manage fuzzing as part of pen testing
- SPIKE - network fuzzing framework

---

# Quiz

The quiz for this week covers all of the material for this week. You must submit the quiz no later than December 8. You will have three attempts to complete the quiz, at two hours per attempt. It consists of 12 questions, and if you are well versed in the material it should take no more than 30 minutes (but longer if you have to go back and look things up, obviously).

# End of Course Survey

Please take several minutes to take a Background survey.
We also want to know your feedback on this course. Please also take the End of Course Feedback Survey. Thanks.

---

# Project

There is no new project for this week. All outstanding projects and assessments are due by 8am EST on December 8.

---

Created Wed 9 Apr 2014 6:16 AM PDT
Last Modified Wed 3 Dec 2014 12:09 PM PST