Breakpoint Training
October 6-7, 2014
Melbourne, Australia

THE EXPLOIT LABORATORY: INTRODUCTION TO EXPLOIT DEVELOPMENT

OVERVIEW

The Exploit Laboratory's introductory course is an all new beginner to intermediate level class, for those curious to dig deeper into the art and craft of software exploitation. We begin with a quick overview of memory corruption and stack overflows and then move on to browser exploits, heap sprays and vtable overwrites. The latter part of the class covers practical examples on defeating modern day exploit mitigation techniques like DEP and ASLR using Return Oriented Programming (ROP).

In addition to core exploit development, the class also focuses heavily on developing debugging skills, performing root cause analysis and negotiating complex obstacles.

The Exploit Laboratory requires a lot of hands on work. Lab examples used in this class feature popular third party applications and products instead of simulated lab exercises.

All topics are delivered in a down-to-earth, learn-by-example methodology. The same trainers who brought you The Exploit Laboratory for over nine years have been working hard in putting together advanced material based on past feedback.

LEARNING OBJECTIVES

- Memory Corruption Bugs - past and present
- Stack Overflows on Linux and Windows
- Browser Exploits
- PDF Exploits
- Heap Spraying in browsers and PDF readers
- Abusing Objects in memory - vftable overwrites
- Exploiting browsers via object corruption
- Introduction to Return Oriented Programming
- Defeating DEP using ROP
- Bypassing ASLR on Windows 7.

DAY 1 SYLLABUS

1. Memory Corruption Bugs - past and present
2. Stack Overflows on Linux and Windows
3. Browser Exploits
4. PDF Exploits
5. Heap Spraying in browsers and PDF readers
6. Abusing Objects in memory - vftable overwrites.

DAY 2 SYLLABUS

1. Exploiting browsers via object corruption
2. Introduction to Return Oriented Programming
3. Defeating DEP using ROP
4. Bypassing ASLR on Windows 7.

ABOUT THE TRAINER

Saumil Shah is the founder and CEO of Net-Square, providing cutting edge information security services to clients around the globe. Saumil is an internationally recognized speaker and instructor, having regularly presented at conferences like Blackhat, RSA, CanSecWest, PacSec, EUSecWest, Hack.lu, Hack-in-the-box and others. He has authored two books titled "Web Hacking: Attacks and Defense" and "The Anti-Virus Book".

Saumil graduated with an M.S. in Computer Science from Purdue University, USA and a B.E. in Computer Engineering from Gujarat University. He spends his leisure time breaking software, flying kites, traveling around the world and taking pictures.

PRE-REQUISITE INFORMATION

Each class has prerequisites for software and a laptop is mandatory. Some classes also require students have prior knowledge. Please check individual class pre-requisites on the website for more information.

Trainer	Saumil Shah
Dates	October 6-7, 2014
Level	Introduction

REGISTRATION FEES

Early Bird	$3,080	Ends June 30, 2014
Regular	$3,300	Ends July 31, 2014
Late	$3,520	Starts August 1, 2014

Prices include GST

Click here for more information or to register for this Breakpoint Training Session
REGISTRATION WILL CLOSE ON SEPTEMBER 5, 2014