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

BREAKPOINT RUXCON

Breakpoint Training
October 6-7, 2014
Melbourne, Australia

OPEN SOURCE INTELLIGENCE AND AUTOMATING INTELLIGENCE COLLECTION

OVERVIEW

This training is designed to give concepts of where to look for open source intelligence and a starting point for analysing and reporting on it in the first day, and developing bare bones automated collection/analysis systems on the second day. At the end of this course the attendees will have a basis for tools that they can use in-house to increase their security maturity.

DAY 1 - INTRODUCTION

- What is Open Source Intelligence?
- Why do we gather intelligence?
- How to set up an intelligence function in your organisation
- Writing intelligence reports
- Establishing covert identities
- Basics of Paterva Casefile/Maltego
- Image metadata
- Basics of IRC and other chat protocols
- Places to look for criminals.

DAY 2 - AUTOMATION

- Introduction to Python
- Helpful frameworks
- Services with APIs
- Looking like a real human
- Web Scraping
- Data storage
- Basic web frontends
- Writing Maltego Transforms.

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.

ABOUT THE TRAINER

Kayne Naughton is a technologist and security researcher with 15 years' experience across the education, government and finance industries.Since 2013 he has been running a start-up, Asymmetric Security, focused on security intelligence for the finance and corporate sector. Kayne is also a volunteer with the Shadowserver Foundation, a US based non-profit dedicated to keeping the internet safe. He is currently focused on researching cyber crime, malware and open source intelligence but draws on experience in system administration, coding and teaching.

Trainer	Kayne Naughton	
Dates	October 6-7, 2014	
Level	Beginner	

REGISTRATION FEES

Early Bird	$2,420	Ends June 30, 2014
Regular	$2,750	Ends July 31, 2014
Late	$3,080	Starts August 1, 2014

Prices include GST

Click here for more information or to register for this Breakpoint Training Session
REGISTRATION WILL CLOSE ON OCTOBER 1, 2014

ADVANCED WEB HACKING

OVERVIEW

Tired of alert(1)? You think there is more to life than running Burp scanner? You went through PentesterLab's exercises and thought "I WANT MORE!!"? This training is for you!

This 2-day training will get you to the next level. We will look into CORS, WebSockets, the exploitation of vulnerabilities published in 2014 (Struts RCE, Rails', Heartbleed...). We will also get shells using serialisation in multiple languages and find vulnerabilities that you may have missed in the past.

After a quick overview of what you need to know to attack web applications, we will directly jump to the interesting stuff: hands-on training and real attacks. The class is a succession of 10 minute explanations on what you need to know, followed by hands-on examples to really understand and exploit vulnerabilities.

After the training, you go home with the course (slides based), the detailed version of the course (in-depth walk-through), and the systems to be able to play and refresh your memory!

SYLLABUS

- Cross-origin resource sharing
- WebSockets
- Struts RCE
- Multiple Serialisation attacks (PHP, Python, Java)
- Jboss web-console
- Blind XML entities attacks
- Heartbleed
- Tricky SQL injections

ABOUT THE TRAINERS

Louis Nyffenegger is an experienced and sought-after security consultant specialising in web penetration testing. He is a regular guest speaker at local security conferences including Ruxcon and Owasp, and has conducted a web application security training at both conferences. In his spare time Louis helps set up Ruxcon's Capture the

Flag competition. In 2011, Louis started PentesterLab, a company specialising in security training. Recently, Louis published Bootcamp, a learning path for getting into penetration testing.

Luke Jahnke is the creator of Bitcoin CTF, one of the hardest CTF dedicated to web security. He is a regular guest speaker at local security conferences. After working as a web developer, Luke moved to security and has been popping shells for several years now.

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.

Trainers	Louis Nyffenegger & Luke Jahnke	
Dates	October 6-7, 2014	
Level	Advanced (Web)	

REGISTRATION FEES

Early Bird	$2,200	Ends June 30, 2014
Regular	$2,530	Ends July 31, 2014
Late	$2,860	Starts August 1, 2014

Prices include GST

Click here for more information or to register for this Breakpoint Training Session
REGISTRATION WILL CLOSE ON OCTOBER 1, 2014