



Exploit Development Courses

Exploit Dev: No Assembly Required Oct 31 - 4 Nov 2011 (5 Days)
Exploit Dev: Target Practice Nov 7 - 11 2011 (5 Days)



Strategic Security Training



Strategic Security has a comprehensive network and application security training program designed to meet the needs of individuals, departments, and organizations to develop highly skilled security professionals.



Table of Contents

Exploit Dev Package Course Description.....	4
Exploit Dev: No Assembly Required & Exploit Dev: Target Practice	4
Course 1 Description.....	5
Exploit Dev: No Assembly Required	5
Course 2 Description.....	7
Exploit Dev: Target Practice.....	7
Training Dates and Times.....	10
Training Costs (with TinyURL payment links)	10
Training Location.....	10
About The Instructor.....	11
About Strategic Security, Inc.	11
Who To Contact For More Information.....	11

Exploit Dev Package Course Description

Exploit Dev: No Assembly Required & Exploit Dev: Target Practice

Strategic Security has teamed up with Net-Square to provide the most comprehensive exploit development course package available to the public. Occasionally similar courses are offered privately to various three letter agencies and large financial institutions.

Exploit development is often considered the most difficult area of focus in the entire field of IT security. It requires both a broad range of skills and deep level of knowledge in Networking, Operating Systems, and Programming. Now you too can learn what has long been thought to be "Black Magic" by many from one of the top practitioners and trainers in the world.

How is this course put together?

The course is actually a 2 week package deal designed to both teach the fundamentals of modern exploit development and give the student ample guided practice time with the instructor to actually get proficient.

Benefits:

- Takes the student from relative beginner in exploit development to writing weaponized exploits against real world applications that run on both 32bit and 64bit architectures and utilize modern exploit mitigations such as DEP, ASLR.
- Is lower priced than other similar courses, and offers much more labs and practice time. The student will learn how to do it instead of just learn about it as in other courses.
- Course is taught by a skilled practitioner, and trainer that is well regarded in the IT Security community.
- Focuses more writing exploits against applications using modern mitigations than other courses.
- Doesn't require the student to know Assembly prior to attending the course



Course 1 Description

Exploit Dev: No Assembly Required

The wildly successful Exploit Laboratory and The Exploit Laboratory: Black Belt Edition are now combined in an all-in-one package that takes you from "n00b" to "1337" in five days. Exploit Dev: No Assembly Required is an intense hands-on class for those wishing to dive into vulnerability analysis, exploit writing and being able to circumvent popular exploit mitigation techniques.

Exploit Dev: No Assembly Required features real world applications as candidates for exploitation rather than building up on carefully simulated lab exercises. Most of the class time is spent working on exploit writing exercises featuring some of the latest applications on Linux, Windows and Mac OS X. All this—delivered in a down-to-earth, learn-by-example methodology, by trainers who have been teaching advanced topics in computer security for over 10 years. This class does NOT require knowledge of assembly language. A few concepts and a sharp mind is all you need.

Course Highlights:

- Stack Overflows (in both Linux and Windows)
- Heap Overflows (in both Linux and Windows)
- Integer Overflows
- Exploits on Mac OS X
- Abusing Structured Exception Handlers on Windows
- Abusing Vectored Exception Handlers on Windows
- Browser Exploits
- PDF Exploits
- Exploits on Mac OS X.
- Defeating DEP using Ret2LibC.
- Introduction to Return Oriented Programming
- ROP gadgets and stack flips.
- ROP shellcode loaders
- Practical ROP Exploits
- Bypassing ASLR on Windows 7
- Kernel exploitation
- JIT spraying
- Advanced browser exploits
- Advanced PDF exploits

Course 1 Outline

Day 1: Smashing the Stack

- * Introduction to systems concepts
- * Using GDB and WinDBG
- * Stack overflows on Linux
- * Stack overflows on Windows XP

Day 2: Heap Overflows and Browsers

- * Introduction to heap exploitation
- * Heap overflows on Linux
- * Heap overflows on Windows
- * Browser exploitation

Day 3: Browsers, PDF and Mac OS X

- * Browser exploitation continued
- * PDF exploits
- * Exploits on Mac OS X
- * Capture-The-Flag Round 1

Day 4: ROP

- * Defeating DEP using Ret2LibC
- * Introduction to Return Oriented Programming
- * Practical ROP exploits
- * Bypassing ASLR
- * Capture-The-Flag Round 2

Day 5: Advanced Topics

- * Complex exploits
- * Kernel exploitation
- * Integer overflows
- * JIT spraying
- * Advanced browser exploits
- * Advanced PDF exploits



Course 2 Description

Exploit Dev: Target Practice

Exploit Dev: Target Practice is a live fire capture the flag style of course that builds on the lessons learned in the previous week. The instructor brings nearly 70 vulnerable live applications to the course and students must craft exploits against these real world applications that run on both 32bit and 64bit architectures and utilize modern exploit mitigations such as DEP, ASLR.

The goal of the first week's course was to teach the fundamentals of modern exploit development. The goal of the second week is to give the students as much practice as possible writing exploits against real world applications. The instructor will be there to provide as much or a little hints, tips and tricks as the student needs.

Remember - the goal here is practice. We want to reinforce what the student learned in the first week as well as provide the student with more time the instructor to really learn the finer points of exploit creation.

Course Highlights:

- Browser Exploits
- PDF Exploits
- Dealing with DEP
- Practical ROP Exploits
- Bypassing ASLR on Windows 7
- Kernel exploitation
- JIT spraying
- Advanced browser exploits
- Advanced PDF exploits

Course 2 Outline

Day 1: Smashing the Stack

- Stack overflows on Windows XP
- Capture-The-Flag

Day 2: Heap Overflows and Browsers

- Heap overflows
- Browser exploitation
- Capture-The-Flag

Day 3: Browsers, and PDF Exploits

- Browser exploitation
- PDF exploits.
- Capture-The-Flag

Day 4: ROP

- Practical ROP exploits.
- Bypassing ASLR.
- Capture-The-Flag

Day 5: Advanced Topics

- Complex exploits
- Kernel exploitation
- Advanced PDF/Browser Exploits
- Capture-The-Flag



Prerequisite Skills:

- Have a working knowledge of operating systems - Win32 and Unix.
- Not be allergic to command line tools.
- Use vi/pico/joe editors.
- Have a working knowledge of shell scripts, cmd scripts or Perl.
- Understanding of C programming would be a bonus.

A workstation with all of the required software for the class will be provided for each student.

Students are allowed to bring their own laptops to class, but they must meet the following requirements.

Hardware Requirements:

- A working laptop (no Netbooks)
- Intel Core 2 Duo x86 hardware (or superior) required
- 2GB RAM required, at a minimum, 4GB preferred
- Wireless network card
- 20 GB free Hard disk space

Software Requirements:

- Windows XP SP3 / Windows 7 / Linux kernel 2.4 or 2.6 / Mac OS X 10.5 or 10.6 (Intel only)
- VMWare Player / VMWare Workstation / VMWare Fusion MANDATORY
- Administrator / root access MANDATORY
- Ability to disable Anti-virus software on your laptop
- Ability to disable Host firewall
- Perl 5.8
- An SSH client, such as PuTTY
- Netcat

NOTE: If your laptop is a locked-down company issued laptop, please make sure you have VMWare Workstation or VMWare Player installed by your administrator before you come to class.

NOTE: Please read the above note SERIOUSLY!



Training Dates and Times

Workshop 1: Oct 31st - Nov 04th, 2011
Workshop 2: Nov 7th - Nov 11th, 2011

The training will be held from 8:30am to 4:30pm each day. The class will be broken down into 50 minute sessions, 10 minute breaks, and 1 hour for lunch each day.

Training Costs (with TinyURL payment links)

Workshop 1:	\$7,000	http://tinyurl.com/SS-EDNAR
Workshop 2:	\$8,000	http://tinyurl.com/SS-EDTP
Workshops 1 & 2	\$12,500	http://tinyurl.com/SS-EDNAR-TP

Defense contractor, Active Duty Military, FBI, CIA, Secret Service, College student, ISSA, ISACA, former ACE student, and Infragard member discounts.

Workshop 1:	\$5,000	http://tinyurl.com/SS-EDNAR-D
Workshop 2:	\$6,000	http://tinyurl.com/SS-D-EDTP
Workshops 1 & 2	\$8,500	http://tinyurl.com/SS-EDNAR-TP-D

Training Location

The workshops will be held at "The Academy of Computer Education" in Greenbelt, MD.

The address is:
7833 Walker Drive, Suite 520C
Greenbelt, Maryland 20770



About The Instructor



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". Before Net-Square, he worked with Foundstone Inc and Ernst & Young in the US, and is currently a guest faculty at the Indian Institute of Management, Ahmedabad for their Management Development Programmes. 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 traveling around the world and taking pictures.

About Strategic Security, Inc.

Strategic Security, Inc., is an IT Security consulting firm that provides in-depth technical security assessments of networks, web applications, and regulatory compliance gap analysis (ex: PCI, HIPAA, ISO 27000, etc). Strategic Security also helps companies by providing them with guidance on integrating security into their software development lifecycle, building an enterprise security program, and much more.

Who To Contact For More Information

You can contact Joe McCray at:

Toll Free: 1-866-892-2132
Email: joe@strategicsec.com
LinkedIn: <http://www.linkedin.com/in/joemccray>
Twitter: <http://twitter.com/joemccray>
Website: <http://strategicsec.com>