Course Syllabus

Assessing and Exploiting Web Applications with Samurai-WTF

Course Abstract

Come take the official two-day Samurai-WTF training course given by one of the founders and lead developers of the project! You will learn the latest Samurai-WTF open source tools and as well as the latest techniques to perform web application penetration tests. After a quick overview of pen testing methodology, the instructors will lead you through the end-to-end process of testing and exploiting several different web applications, including client side attacks using flaws within the application. Different sets of open source tools will be used on each web application, allowing you to learn first hand the pros and cons of each tool. Primary emphasis of these instructor lead exercises is how to integrate these tools into your own manual testing procedures to improve your overall workflow. After you have gained experience with the Samurai-WTF tools, you will be challenged with a capture the flag event. This final challenge will give you time to practice your new skills at your own pace and experiment with your favorite new tools. This experience will help you gain the confidence and knowledge necessary to perform web application assessments and expose you to the wealth of freely available, open source tools.

Instructor Bio

Justin is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and currently plays key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), National Electric Sector Cybersecurity Organization Resources (NESCOR), and Smart Grid Interoperability Panel (SGIP). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences, and is currently an instructor for the SANS Institute. In addition to electric power industry conferences, Justin frequently presents at top security conferences such as Black Hat, DEFCON, OWASP, and AusCERT. Justin co-leads prominent open source projects including the Samurai Web Testing Framework, Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

Instructor Contact Information

Justin Searle, Managing Partner – UtiliSec
Personal: justin@meeas.com // Work: justin@utilisec.com
Cell: +1 801-784-2052
http://twitter.com/meeas
http://www.linkedin.com/in/meeas

Course Objectives

1. Attendees will be able to explain the steps and methodology used in performing web application assessments and penetration tests.
2. Attendees will be able to use the open source tools on the Samurai-WTF CD to discover and identify vulnerabilities in web applications.
3. Attendees will be able to exploit several client-side and server-side vulnerabilities.

Course Prerequisites

A basic understanding of web application vulnerabilities and attacks is assumed. This course will focus on use of the tools and their integration into your manual testing procedures, not the theories behind the attacks. This course is designed for novice to intermediate level security professionals, be they developers, managers, or penetration testers.

Resources Your Responsible to Bring

1. Laptop with a functional DVD drive
2. Latest VMware Player, VMware Workstation, or installed
3. Ability to disable all security software on their laptop such as Antivirus and/or firewalls
4. Four (4) GB of hard drive space
5. At least two (2) GB of RAM

Resources Provided at the Course

1. Power for your laptop
2. Bootable DVD with special pre-release version of Samurai-WTF (ISO file available upon request)
3. PDF version of the slide deck

Concepts and Tools Covered

Samurai-WTF Project and Distribution
- About the Project
- Using the Live-DVD
- Joining the Project

Web Application Assessment Methodology
- Pentest Types and Methods
- Formal Four Step Methodology
- Overview of Web Applications Security Vulnerabilities

Reconnaissance Tools Overview

Mapping Tools
- Overview of Mapping
- Port Scanning and Fingerprinting (Labs: nmap, zenmap, Yokoso!)
- Web Service Scanning (Labs: Nikto)
- Spidering (Labs: wget, curl, Zed Attack Proxy, WebScarab, BurpSuite)
- Discovering "Non-Discoverable" URLs (Labs: DirBuster)

Discovery Tools
- Using Built-in Tools (Labs: Page Info, Error Console, DOM Inspector, View Source)
- Poking and Prodding (Labs: Default User Agent, Cookie Editor, Tamper Data)
- Interception Proxies (Labs: Zed Attack Proxy, WebScarab, BurpSuite)
- Semi-Automated Discovery (Labs: Zed Attack Proxy, Rat Proxy)
- Automated Discovery (Labs: Zed Attack Proxy, w3af)
- Dictionary File Creation (Labs: CeWL)
- Fuzzing (Labs: Zed Attack Proxy, JBroFuzz, BurpIntruder)
- Finding XSS (Labs: TamperData, Zed Attack Proxy)
- Finding SQL Injection (Labs: Zed Attack Proxy, sqlmap)
- Decompiling Flash Objects (Labs: Flare)

Exploitation Tools
- Username Harvesting (Labs: Raft)
- Brute Forcing Passwords (Labs: Raft)
- Command Injection (Labs: w3af)
- Exploiting SQL Injection (Labs: SQLMap, Laudanum)
- Exploiting XSS (Labs: BeEF & BeEF Ruby)
- Advanced exploitation through tool integration (Labs: Zed Attack Proxy + sqlmap, BeEF + Metaspliot)