Penetration Testing Made Easy

Abstract: This comprehensive hands on penetration testing course will give you hands on experience in many facets of information security. In this course we will cover a broad ranges of topics to create a good jumping off point for future studies or research in security. This course is ideal for security beginners who are not quite sure what their specialty will be. We will cover penetration testing networks and web applications. Starting with information gathering, we will move through all phases of penetration testing. We will touch on the basics of attacking wireless networks. We will cover exploit including stack overflows and SEH overwrites. We will look at reverse engineering simple programs and get familiar using IDA Pro. Finally, we will take a look at the rapidly developing field of mobile hacking. The course will finish with a live capture the flag environment where students can test what they have learned.

Outline:

Module 1: Using the Metasploit Framework

The Metasploit Framework

Using Msfconsole

Using Msfcli

Using Msfvenom

Module 2: Reconnaissance and Information Gathering

Passive Reconnaissance

OSINT

Maltego

Port Scanning

Nmap

Metasploit Port Scanners

Module 3: Vulnerability Analysis

Vulnerability Scanning

Nessus

Nmap Scripting Engine

Nikto

Metasploit Vulnerability Scanners

Manual Analysis

From Scanner Results to Exploits

Module 4: Exploitation

Exploiting Windows Vulnerabilities

Exploiting Linux Vulnerabilities

Exploiting Website Vulnerabilities

Exploiting Misconfiguration Issues

Module 5: Post Exploitation

Metasploit's Meterpreter

Pivoting

Password Cracking

Getting Domain Admin

Maintaining Access

Reporting

Module 6: Assessing Custom Web Applications

SQL Injection

Cross Site Scripting

Cross Site Request Forgery

Insecure Direct Object Reference

Broken Session Management

Broken Access Controls

Bad Cryptography

Module 7: Advanced Exploitation

Client Side Attacks

Bypassing Antivirus

Social Engineering

The Social Engineer Toolkit

Module 8: Wireless Assessments

Wardriving

Attacking WEP

Attacking WPA/WPA2

Module 9: Exploit Development Part 1

Ollydbg

Setting Up the Environment

A Simple Stack Overflow Exploit on Linux

Writing an exploit for a Windows stack overflow vulnerability

Module 10: Exploit Development Part 2

Fuzzing

An SEH Overwrite Exploit

Metasploit Module Structure

Writing an Auxiliary Module

Porting an Exploit into Metasploit

Module 11: Reverse Engineering

IDA Pro

Setting Up The Environment

Reversing a Simple Binary

Module 12: Capture the Flag

Instructor Bio:

Georgia Weidman is a penetration tester, security researcher, and trainer. She holds a Master of Science degree in computer science, secure software engineering, and information security as well as holding CISSP, CEH, NIST 4011, and OSCP certifications. Her work in the field of smartphone exploitation has been featured in print and on television internationally. She has presented her research at top conferences around the world including Shmoocon, Blackhat, Hacker Halted, and Bsides. Georgia has delivered highly technical security training for conferences, schools, and corporate clients to excellent reviews. Building on her experience, Georgia founded Bulb Security LLC (http://www.bulbsecurity.com), a security consulting firm specializing in security assessments/penetration testing, security training, and research/development. She was awarded a DARPA Cyber Fast Track grant to continue her work in mobile device security, culminating in the release of the Smartphone Pentest Framework (SPF) which allows pentesters to assess the security of mobile devices in an environment.