WASTC 2018 Faculty Development Weeks

Penetration Testing with Kali

Dates: In Person, June 18 - 23, 2018 @ Coastline College, Garden Grove, CA

Advanced techniques of defeating computer security, and countermeasures to protect Windows and Unix/Linux systems. Hands-on labs include Google hacking, automated footprinting, port scans, privilege escalation, attacks against telephone and Voice over Internet Protocol (VoIP) systems, routers, firewalls, wireless devices, Web servers, and Denial of Service attacks. This course helps students to prepare for Offensive Security Certified Professional (OSCP) certification.

By the end of the course, students will be prepared to:

- Use Google and automated footprinting tools to locate vulnerable Web servers, passwords, open VNC servers, database passwords, and Nessus reports
- Perform port scans with several tools, and protect servers from the scans
- Enumerate resources on systems using banner-grabbing and specific attacks against common Windows and Unix/Linux services including FTP, Telnet, HTTP, DNS, and many others, and protect those services
- Use authenticated and unauthenticated attacks to compromise Windows and Unix/Linux systems and install backdoors and remote-control agents on them, and protect the systems from such attacks
- Enter networks through analog phone systems, defeating many authentication techniques, and defend networks from such attacks
- Penetrate PBX, voicemail, Virtual Private Network (VPN), and Voice over Internet Protocol (VoIP) systems, and defend them
- Perform new wireless attacks, including denial-of-service and cracking networks using Wi-Fi Protected Access (WPA) and WPA-2
- Identify firewalls and scan through them

- Perform classical and modern Denial of Service (DoS) attacks, and defend networks from them
- Locate Web server vulnerabilities, exploit them, and cure them
- Describe many ways Internet users are attacked through their browsers and other Internet clients, and the protective measures that can help them
- Student Learning Outcomes (measured to guide course improvements)
- Enumerate resources on systems using banner-grabbing and specific attacks against common Windows and Unix/Linux services including FTP, Telnet, HTTP, DNS, and many others, and protect those services
- Perform classical and modem Denial of Service (DoS) attacks, and defend networks from them
- Locate Web server vulnerabilities, exploit them, and cure them

Prerequisites: Familiarity with security concepts at the Security+ level. Prior experience with Linux is helpful but not required.

Recommended Textbook: Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman -- ISBN-10: 1593275641, No Starch Press; 1 edition (June 8, 2014)

Instructor: Sam Bowne, Ph.D.

Sam Bowne has been teaching computer networking and security classes at CCSF since 2000. He has given talks and hands-on trainings at DEFCON, HOPE, B-Sides SF, B-Sides LV, BayThreat, LayerOne, Toorcon, and many other schools and conferences.

Degrees: B.S. in Physics from Edinboro University of Pennsylvania and a Ph.D. in Physics from University of Illinois, Urbana-Champaign.
Certificates: Current CISSP; older certificates from Cisco, Juniper, Microsoft, and others..

Sponsored by:

WESTERN ACADEMY
SUPPORT & TRAINING CENTER