Hands on Penetration Testing with BackTrack 3

0wning the network

Overview:

This is an intensive, hardcore, hands on Security class by the creators of Backtrack especially designed for delivery in BlackHat Trainings. The course is an interesting amalgamation between our entry level course (“Offensive Security 101”) and expert level course (“BackTrack to the Max”).

A professional and seasoned team of Security Professionals will help you take your skills a few steps further. "Common" hacking techniques are revisited from a professional and practical approach for a better and more efficient pentest. Several topics include "hardcore drilldowns", such as bypassing ASLR during exploit development, injecting malicious code into files under Windows Vista, bypassing Antivirus systems, etc - all based on the award winning live Distribution - BackTrack 3. The course is heavily laced with the “do it yourself” approach, and will expose you to the raw underlying mechanisms of the various attack vectors.

In addition, commercial penetration testing software such as Core Impact and Saint Exploit will be explored in a controlled lab environment. Complimentary demos will be handed out to students.

Lab Description

This course includes complex hands on labs throughout the training. All students will be provided with pre-configured VMware machines for the duration of the course for a personal and in depth learning experience. We will break Windows 2000, XP SP2, Vista and Cisco – all using a special version of BackTrack 3 specially designed for this course.

Who should attend?

"Hands on Penetration testing with BackTrack 3" is a highly technical course aimed at security professionals. People with entry level "hacking" security certifications in need of modern and practical real world penetration testing experience and insights should attend. This is not an entry level course. Students are expected to be familiar with the basic methods and methodologies of an attack as a prerequisite.

Prerequisites:

- Students need to be comfortable in Linux - We'll be using BackTrack during the whole course as our attacking platform. Navigating through directories, executing scripts and tools and writing basic bash scripts are the basic skills expected from the student.
- A solid understanding of TCP/IP and various network services (DNS, DHCP, etc)
- A fair understanding of penetration testing methodology and familiarity with common tools and attacks.
- An understanding of the mechanisms behind Win32 Buffer Overflows.
- Knowledge of a scripting language (Perl, Python, Ruby) is recommended, but not required.

What to bring:

- Students are required to bring their own laptops with a minimum 1 GB RAM installed.
- VMware Server / Workstation (latest edition) installed.
- At least 60 GB HD free
- CDROM / USB support

Topics Covered:

- Scripting your way through backtrack
- Advanced information gathering techniques
- Kung fu Port Scanning
- ARP Spoofing - dynamic manipulation of traffic
- Fuzzing with spike
- Basic shellcode development
- Developing exploits under recent Windows Systems (XPSP2, Vista)
- Developing client side attacks
- Advanced password attacks
- Web application attacks on steroids.
- Working with exploits in BackTrack
- Exploit frameworks
- Backdooring PE files under Windows Vista
- Advanced Trojan development
- AntiVirus Avoidance

Course Length:

Four days. All course materials, custom BackTrack CD's, lunch and two coffee breaks will be provided. A Certificate of Completion will be offered.

Trainer:

Mati Aharoni

Mati is the core developer of the BackTrack liveCD and an active member in remote-exploit.org. Mati is a seasoned security professional with over 10 years of experience as a professional penetration tester. Mati has uncovered several major security flaws and is actively involved in the offensive security arena. In addition, he is the lead trainer and developer of the internationally acclaimed security courses, Offensive Security 101, WIFU and BackTrack to the Max.