

**Workshop Guru**



Workshop 1

Web Application Hacking *LIVE*

This is a revolutionary web application hacking workshop with complete hands-on experience, covering the entire process of hacking web applications inside out.

The workshop aims to provide developers and programmers the best understanding on web application security, with in depth experimentation on the important aspects in web application such as application mapping authentication, access control, injection flaws and advanced exploitation.

Participants learn the essential knowledge on web application security testing and all the advanced techniques for finding and countermeasures security threats in applications.

Scope of Training Includes:

- Anatomy of cross-site scripting attack
- SQL Injection vs Oracle, MySQL and MSSQL
- Authenticating the non-authenticable
- Interpreting the injections (LDAP, XPath, SOAP and other injection)
- And more...

Who Should Attend

This cutting-edge, hands-on workshop is aimed at Information Security Professionals who want to learn in-depth about web application exploits and how to defend them.

Lab requirement

A working laptop with the following hardware/software requirements:

- Pentium IV or better processor • At least 1 GB RAM
- 10 GB free hard drive space • Wireless capability
- CD/DVD drive • Windows XP
- Microsoft Office • Adobe Acrobat Reader
- Machines should NOT contain any personal or company data

Pre-Requisite

Students should be familiar with the following web technologies and programming languages:

- HTTP
- HTML
- Javascript
- ASP
- PHP
- SQL

Each student must bring his own laptop with Windows XP/Vista or a recent Linux distribution such as:

- Fedora
- RHEL
- Gentoo
- Ubuntu





Workshop 2

Penetration Testing Highly Secured Environments *LIVE*

This training will focus on penetration testing techniques that can be used when testing highly secured environments. If you are tired of attacking unpatched Windows 2000 Servers in your hacking courses and want to take a course where you will be attacking new Operating Systems/Applications that are patched, locked down, and protected with an IDS/IPS then this is the course for you.

The highly technical training will cover attacking heavily protected environments from the outside and dealing with Network-Based IDS/IPS, attacking web applications and dealing with Load Balancing, common application security measures in PHP/ASP.NET, Web Application Firewalls, attacking from the LAN, dealing with NAC solutions, locked down workstations/GPOs, and Host-Based IDS/IPS.

Scope of training includes:

- Advanced Scanning
- Stealth Scanning
- Attacking From the Web
- Client-Side Pentesting
- Attacking From the LAN
- Breaking out of Restricted Environments
- Bypassing Network-Based IDS/IPS
- Privilege Escalation
- Post-Exploitation

Who Should Attend

This workshop will significantly benefit security officers, auditors, security professionals, site administrators, network server administrators, firewall administrators, security testers, system administrators, risk assessment professionals and security analysts.

Lab requirement

A working laptop with the following hardware/software requirements:

- Pentium IV or better processor
- At least 1 GB RAM
- 10 GB free hard drive space
- Wireless capability
- CD/DVD drive
- Windows XP
- Microsoft Office
- Adobe Acrobat Reader
- Machines should NOT contain any personal or company data

Pre-Requisite

Students that are Network/System Administrators with three (3) or more years experience working in environments such as financial institutions, DoD networks, or similar high security environments will benefit greatly from this course. It is however primarily designed for Network/Web Application Penetration testers that are looking for the little tips and tricks that will help them better attack high security environments.

Students must be familiar with IT Security best practices, and have a good understanding of TCP/IP and common web technologies.

- Basic Windows administration for servers and workstations
- Basic Linux/*NIX system administration skill
- Basic command line proficiency on both Windows and *NIX systems

Students should be familiar with the following web technologies and languages:

- HTTP
- HTML
- Javascript
- ASP
- PHP
- SQL





Workshop Guru



Workshop 3

E-Crime Investigation *LIVE*

This workshop enables the participants entering an exciting and challenging virtualized cyber crime investigation scenario. Using task orientated approach; participants will go through a series of simulated hacking incidents, interactively supported by the trainer.

The core of the workshop is to provide the participants a real world experience to learn and utilize digital forensic analysis technique and mythologies with a strong emphasis on technical understanding and skills. At the end of the workshop, participants will need to explore and investigate a mysterious cyber criminal scenario with application of all investigation skills learned in the workshop.

Scope of Training Includes:

- Employing sophisticated investigation skills and highly developed forensic tools in real world investigation scenario
- Steganography analysis
- Entire forensic process with hardware and software acquisition
- Network Forensic investigation
- And more...

Who Should Attend

This cutting-edge, hands-on workshop is aimed at Information Security Professionals who requires effective digital forensic investigation skills; more specifically targeting audiences like Corporate Security Officers, System Administrators, Law Enforcement Officers and Ethical Hackers.

Lab requirement

A working laptop with the following hardware/software requirements:

- Pentium IV or better processor • At least 1 GB RAM
- 10 GB free hard drive space • Wireless capability
- CD/DVD drive • Windows XP
- Microsoft Office • Adobe Acrobat Reader
- Machines should NOT contain any personal or company data

Pre-Requisite

Students should be comfortable using Linux as an operating environment. Students must supply their own laptop with a Linux installation, including X windows. This installation can be either native, or in VMware. The Linux installation must have at least 300 MB of free space. Development tools (e.g. gcc, make, etc.) must be installed on the laptop, however no development experience is required. All tools will be provided on DVD-ROM.

