

Hands-On Ethical Hacking Workshop

About Tranchulas

Tranchulas is an international consulting firm that focuses on Information Security. We are global provider of information security assessment, compliance and managed security services. Tranchulas helps protect enterprises and government organizations by providing customized information security services that meet their business needs.

Addressing the Need

The need to understand hacker and his methods are vital for better defending networks. This workshop is designed for students who want to get acquainted with the world of hacking.

In this industry standard workshop on ethical hacking, students will learn step-by-step procedures for executing Internet, intranet, and host-level security. Tranchulas Hands-on Ethical Hacking is the definitive training regimen for developing countermeasure strategies, such as performing attack and penetration assessments. The hands-on workshop provides real world security knowledge designed to show, through ethical hacking techniques, how real attacks are planned and perpetrated.

About the Workshop

Because security is an ever-changing battlefield, Tranchulas Hands-on Ethical Hacking exposes you to the latest in network and application vulnerabilities and defenses. Our instructor will illustrate

each technology's default security posture, installation weaknesses, methods hackers use to circumvent "secure" settings, and countermeasures for each vulnerability.

Tranchulas instructor will walk you through foot-printing an organization's Internet presence to show you how to identify, exploit, and secure popular and little-known vulnerabilities.

About the Trainer

Zubair Khan is CEO at Tranchulas. He is also Information Security Consultant at NADRA (National Database and Registration Authority) of Pakistan where he is responsible for penetration testing of homeland security solutions like Automated Border Control, Multi-biometric E-Passport etc. He is also responsible for securing National data warehouse. Zubair has been researching mainly on cyber warfare and on various other facets of information security for the past seven years. He has conducted large enterprise security assessments and given information security consultancy to top organizations of Pakistan.

Zubair has conducted security trainings at various forums in Pakistan and abroad. He has previously presented at renowned security conferences including Hack.lu Luxembourg, Hack In The Box Malaysia and Infosek Slovenia. Chairman of Pakistan Engineering Development Board and Chairman of Pakistan Engineering Council recognize his research and work. Zubair holds a bachelor's degree in Business IT from Curtin University of Technology, Australia. He is CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager) and also ISO27001 ISMS (Information Security Management System) Auditor.

Course Outline

- **Introduction to Ethical Hacking and BackTrack**
- **Basic Bash Scripting**
- **Information Gathering**
 - Google Hacking and Harvesting
 - Netcraft
 - DNS Reconnaissance
 - Forward/reverse lookup bruteforce
 - SNMP reconnaissance
 - Enumerating Windows Users
 - Enumerating open TCP ports
 - Enumerating Running Services
 - SMTP reconnaissance
 - Netbios Information Gathering
- **Port Scanning**
 - TCP Port Scanning Basics
 - Nmap
- **ARP Spoofing**
 - DNS Spoofing
 - Traffic Forgery
 - SSL Man In the Middle
- **Buffer Overflow Exploitation**
 - Fuzzing
 - Controlling EIP
 - Shellcode creation
- **Hacking your way through NetCat**
 - Bind Shells and Reverse Shells
- **Exploitation**
 - Compiling and Executing Linux and Windows exploits
 - Exploit Frameworks
 - Writing Metasploit modules
- Metasploit Command line interface
- Meterpreter Payloads
- Binary Payloads
- Framework 3 Auxiliary Modules
- Client side Attacks
- Cisco Exploits
- Trojan and Rootkit Development
- **Password Attacks**
- **Messing with Ports**
 - Port Redirection
 - SSL Encapsulation
 - SSH Tunneling
- **Web Application Hacking**
 - Introduction to Web Scripting
 - Web Application Threats
 - Cross-Site Scripting
 - SQL Injections
 - Enumerating DBs
 - Blind SQL Injections
 - Command Injection Flaws
 - Cookie/Session Poisoning/Hijacking
 - Parameter/Form Tampering
 - Buffer Overflow
 - Directory Traversal/Forceful Browsing
 - Website Defacement through shell programming
- **Wireless Hacking**
 - WEP and WPA Cracking

*Tranchulas Private Limited
2nd Floor, Evacuee Trust Complex,
Sir Agha Khan Road, F-5/1
Islamabad, 44000
PAKISTAN*

*Phone: +92-51-2871433
Email: info@tranchulas.com*