Hands-On Penetration Testing Training Course

About Tranchulas

Tranchulas is a multinational information security company having its offices in UK, USA, New Zealand and Pakistan. We are global provider of information security assessment, compliance, managed security and training 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 training course is designed for students who want to get acquainted with the world of hacking.

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

About the Trainer

Zubair Khan is CEO at Tranchulas. He 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. 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.

Audience

- Penetration Testers
- Information Security Managers
- Information System and Security Auditors
- IT Security specialists
- System and Network Administrators
- Anyone who may be interested in ethical hacking

Pre-Requisites

- Basic knowledge of TCP/IP
- Participants must bring their own laptops

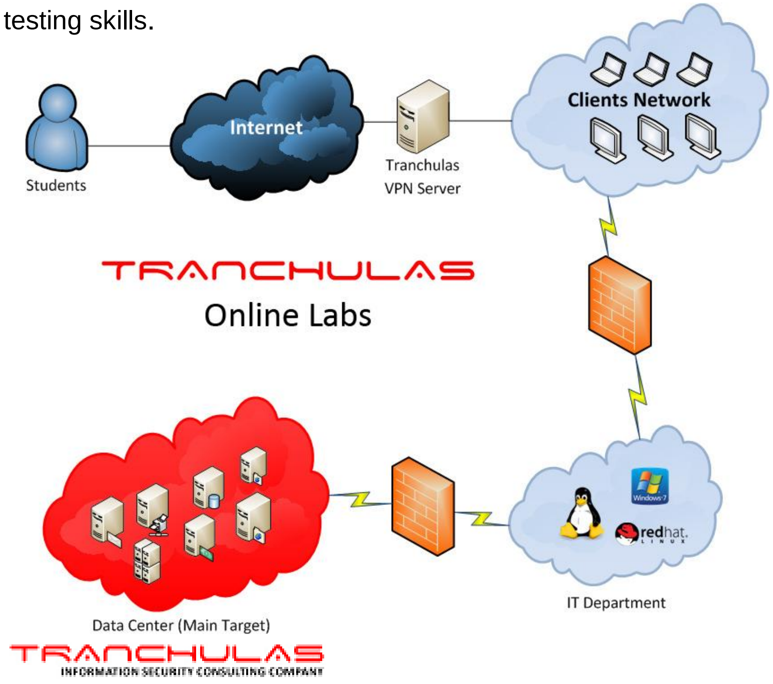
Tranchulas Online Labs

Tranchulas Online Labs are available 24x7 over VPN for practicing the techniques and tools demonstrated by our instructors during the training course. Online labs simulate corporate network with several subnets, each protected by firewall. All machines on the network can be exploited and have different difficulty levels. Students are required to discover and exploit vulnerabilities in order to pass online labs and receive Tranchulas Certified Penetration Testing Professional (CPTP) Certification.

CPTP Certification

This course leads to Tranchulas **Certified Penetration Testing Professional (CPTP)** certification. CPTP is an exclusive certification awarded by Tranchulas UK Ltd, which will test your technical skills in a live network where you are expected to discover and exploit security vulnerabilities. Students are required to pass our online labs in order to receive CPTP.

You can connect with **Tranchulas Online labs for 90 days** to practice your hacking kung-fu after the training course. During this time our technical team will provide you **email/phone/skype support** in order to ensure the skills acquired on the training course are being applied correctly. This will also assist you in resolving questions that have arisen in the workplace after applying newly acquired penetration testing skills.



Course Outline

Module 1: Penetration Testing Planning and Scoping

- Types of penetration testing and ethical hacking projects
- Penetration testing methodology
- Limitations and benefits of penetration testing
- Scoping and time estimation of penetration testing project
- Defining rules of engagement
- Pre and Post Engagement Checklist
- Legal implications of penetration testing
- Exercise: Attendees will find gaps in pre-engagement activities of a penetration testing project

Module 2: Basic Usage of Linux and its services

- Basics of Linux Bash Shell
- Linux Services including DHCP, Apache, SSHD, VNC Server and TFTPD
- Exercise: Attendees will start, stop and test services
- Basic Bash Scripting
- Exercise: Attendees will write a simple bash script

Module 3: Information Gathering

- Google Hacking
- Netcraft
- Whois Reconnaissance
- DNS Reconnaissance
- Forward/reverse lookup bruteforce
- Email Harvesting
- SNMP Reconnaissance

- Exercise: Attendees will identify and enumerate computers running SNMP service on Tranchulas Online Labs
- SMTP reconnaissance
- Netbios Information Gathering
- Exercise: Attendees will identify and gather usernames of machines running SMB service on Tranchulas Online Labs
- Maltego
- Exercise: Attendees will gather information and build a organizational profile using discussed resources in this module

Module 4: Port Scanning

- Port Scanning Basics
- Scanning Techniques
- Nmap - Port Scanning, Network sweeping, OS fingerprinting, Service enumeration, Version scans
- Exercise: Packet crafting with Hping3
- Nmap Scripting Engine
- Exercise: Attendees will use Nmap Scripting Engine to find vulnerabilities
- Firewall/IDS evasion techniques – Fragmentation, Decoys, Timing, Using source ports
- UnicornScan
- Exercise: Attendees will identify live hosts, OS versions, open ports and services along with their version numbers of all machines on Tranchulas Online Labs

Module 5: Sniffing & Man In The Middle Attacks

- ARP Spoofing
- DNS Spoofing
- SSL Man In the Middle
- Traffic Forgery
- Exercise: Create custom Ettercap filter

Module 6: Vulnerability Assessment

- Configuring and Scanning with Open Vulnerability Assessment System (OpenVAS)
- Assessing vulnerabilities using Nessus
- Nexpose vulnerability scanner
- Exercise: Comprehensive vulnerability scanner configuration

Module 7: Buffer Overflow Exploitation

- Fuzzing
- Controlling EIP
- Shellcoding - Shellcode encoding, Windows Command Execution Shellcode, Connectback Shellcode
- Exercise: Create basic shellcode
- Exercise: Exploiting Buffer Overflows

Module 8: Exploitation

- Connecting and listening on TCP/UDP port with Netcat
- Exercise: Create Bind Shell, Reverse Shell and transfer files using Netcat
- Compiling and Executing Linux and Windows exploits
- Exercise: Attendees will attempt to exploit a target machine on Tranchulas Online Labs by fixing, compiling and executing given exploit code
- Metasploit Framework Fundamentals
- Using Metasploit Exploits
- Types of Payloads
- Metasploit Auxiliary Modules
- Exercise: Attendees will use Metasploit to get remote shell of target servers on Tranchulas Online Labs

- Meterpreter Payload
- Exercise: Advance usage of Meterpreter
- Exercise: Writing Metasploit modules

Module 9: Client Side Exploitation

- Binary Payloads
- Bypassing Antivirus
- Exercise: Attendees will create a binary payload and prevent its detection by antivirus through various encoding techniques
- VBScript Infection
- Java Applet Infection
- DLL Hijacking
- PDF Exploits
- Exercise: Compromise target machines by client side exploitation
- Trojan and Rootkit Development
- Exercise: Attendees will create a windows rootkit
- Cisco Exploits
- Armitage Exploitation
- Browser Autopwn
- Social Engineering Toolkit
- Spear Phishing Attacks
- Credential Harvesting Attack
- Tabnabbing Attack
- Web Jacking Attack
- Infectious USB/DVD/CD attack
- Fast Track
- Exercise: Attendees will plan and execute attacks discussed in this module on Tranchulas Online labs

Module 10: Post Exploitation

- Privilege Escalation
- Exercise: Attendees will attempt to gain SYSTEM level privileges on remote system.
- Cleaning event logs
- Persistent Backdoor
- Enabling Remote Desktop
- Exercise: Create backdoor by a script to enable remote desktop and create user account
- Packet sniffing on compromised machines
- Pivoting
- Exercise: Attendees will route traffic from non-routable network

Module 11: Password Attacks

- Online Password Attack
- Exercise: Attendees will write a username/password brute force script
- Exercise: Attendees will crack various authentication based services in Tranchulas Online Labs through Hydra
- Offline Password Attacks
- Exercise: Attendees will exploit Windows server and Linux machines on Tranchulas Online Labs and dump local user password hashes. They will then crack those hashes using John the Ripper or Rainbow tables

Module 12: Messing with Ports

- Port Redirection
- SSL Encapsulation
- SSH Tunneling

Module 13: Web Application Hacking

- Introduction to Web Scripting

- Web Application Threats
- Exercise: Web Vulnerability Assessment
- Cross-Site Scripting
- SQL Injections
- Blind SQL Injections
- Enumerating DBs
- SQLPwnag
- Exercise: Get a shell by exploiting Microsoft SQL based web application
- Command Injection Flaws
- Cookie and Session Poisoning/Hijacking
- Parameter/Form Tampering
- Directory Traversal/Forceful Browsing
- Website Defacement through shell programming
- Exercise: Attempt attacks discussed in this module on different web applications running on Tranchulas Online Labs

Module 14: Wireless Hacking

- WEP Cracking
- WPA Cracking
- Exercise: Attendees will crack WEP and WPA Wireless Networks
- Exercise: Capture passwords and conduct browser based attacks against clients by faking access points

Module 15: Writing a Penetration Testing Report

- Dradis Framework

Contact Tranchulas

United Kingdom

Tranchulas Ltd
Suite 15091, 2nd Floor, 145-157 ST John Street
London, England, EC1V 4PW
Tel: +44 (20) 755-88924

United States

Tranchulas LLC
1 Hallidie Plaza
2nd Floor
San Francisco, CA
94102
Tel: +1 (415) 689-9588

New Zealand

Tranchulas Ltd
Suite 5111, 17B
Farnham Street
Parnell Auckland
1052
Tel: +64 (9) 889-0224

Pakistan

Tranchulas Pvt Ltd
2nd Floor, Evacuee Trust Complex
Sir Agha Khan Road, F-5/1
Islamabad, 44000
Tel: +92 (51) 287-1433

General Inquires: info [at] tranchulas [dot] com

Training Services: training [at] tranchulas [dot] com