TRANCHULAS

Hands-On Ethical Hacking and Penetration Testing Training Course

Introduction

This hands-on training course provides a comprehensive collection of live demonstrations showcasing a wide range of hacking techniques and defensive strategies employed by cyber attackers and security professionals. Participants will gain practical experience through Tranchulas' 24/7 online labs, which are designed to support continuous practice of the methods and tools demonstrated by the instructor during the course. This immersive environment ensures learners can reinforce their skills and confidently apply them in real-world scenarios.

Accreditations

Tranchulas Hands-On Penetration Testing and Ethical Hacking training course is Assured Training in association with the National Cyber Security Centre (NCSC), UK. The course material has been rigorously assessed against the exacting standards of NCSC.

The quality of the trainers' delivery and the course administration has been quality checked and approved by APMG.

Additionally, Tranchulas is CREST Cyber Training Provider, further validating the excellence and credibility of our training offerings.

Course Objectives

By the end of this course, participants will be able to:

1. Understand the fundamentals of ethical hacking, penetration testing methodologies, and best practices.
2. Apply advanced OSINT and reconnaissance techniques to discover critical information about targets.

3. Exploit common and modern vulnerabilities across multiple platforms (Windows, Linux, Web Applications, Active Directory, Cloud).
4. Pivot and escalate privileges within compromised systems and networks using current exploitation techniques.
5. Assess containerized and cloud-based environments for misconfigurations and vulnerabilities.
6. Report findings effectively using industry-standard frameworks and tools, communicating risks to both technical and non-technical stakeholders.

CPTP CERTIFICATION

This course leads to the **Tranchulas Certified Penetration Testing Professional (CPTP)** certification. The CPTP exam tests your ability to discover and exploit security vulnerabilities in a live network environment. To earn the certification, you must successfully complete our online labs.

Course Outline

Module 1 – Penetration Testing Planning & Scoping

- **Learning Objectives**
  - Recognize various penetration testing types (black-box, white-box, grey-box).
  - Outline methodologies (OWASP, PTES, NIST) for structured penetration tests.
  - Clarify scope, timing, and Rules of Engagement.
  - Understand legal and ethical considerations.
  - Prepare comprehensive pre- and post-engagement checklists.
- **Topics Covered**
  - Penetration testing benefits, challenges, and planning guidelines
  - Defining clear Rules of Engagement
  - Scoping and timing estimation
  - Legal aspects and obligations

Module 2 – Basic Usage of Linux and Its Services

- **Learning Objectives**
  - Master fundamental Linux bash shell commands.
  - Manage and test commonly used Linux services.
  - Write simple bash scripts to automate tasks.
- **Topics Covered**
  - Linux Bash Shell basics
  - Starting/stopping services: DHCP, Apache, SSHD, VNC, TFTP
  - Basic Bash scripting exercises

Module 3 – Information Gathering (OSINT)

- **Learning Objectives**
  - Employ advanced OSINT tools and techniques to gather data on targets.
  - Enumerate target networks, domains, and user information effectively.
- **Topics Covered**
  - Google Dorking
  - LinkedIn Profiling & social media recon

- Username Enumeration
- SMB Enumeration
- Whois & DNS Recon (forward/reverse lookups, bruteforce)
- GitHub Recon & theHarvester (optional advanced OSINT)
- Internal live hosts discovery
- **Exercise**: Combine Google Dorking and various techniques for real-world reconnaissance

Module 4 – Sniffing & Man-in-the-Middle Attacks

- **Learning Objectives**
  - Understand packet capture and interception techniques.
  - Execute ARP and DNS spoofing to hijack network traffic.
  - Create and apply custom network filters or injections.
- **Topics Covered**
  - ARP Spoofing
  - DNS Spoofing
  - SSL Man-in-the-Middle
  - Traffic Forgery
  - Ettercap vs. Bettercap (modern MITM frameworks)
  - **Exercise**: Create a custom filter (e.g., with Bettercap or Ettercap) to manipulate traffic

Module 5 – Port Scanning

- **Learning Objectives**
  - Map networks using active scanning techniques.
  - Use Nmap scripting and evasion techniques effectively.
  - Compare multiple scanners (Unicornscan, Rustscan) for efficiency.
- **Topics Covered**
  - Host discovery with Nmap
  - Port scanning and OS fingerprinting
  - Nmap Scripting Engine (NSE) usage
  - Firewall/IDS evasion (fragmentation, decoys, custom ports)
  - Unicornscan and Rustscan
  - **Exercise**: Identify live hosts, OS versions, and open ports/services on Tranchulas Online Labs

Module 6 – Enumeration

- **Learning Objectives**
  - Enumerate key network services to gather deeper insights.
  - Leverage toolsets to systematically identify potential attack vectors.
- **Topics Covered**
  - Enumeration principles and methodologies
  - Enumerating FTP, SMB, NFS, DNS, SMTP, SNMP, Databases (MySQL, MSSQL, Oracle, etc.)
  - **Exercise**: Fingerprint services running on multiple lab machines

Module 7 – Vulnerability Assessment

- **Learning Objectives**
  - Conduct automated vulnerability scans and interpret results.
  - Understand CVSS/CVE standards for vulnerability prioritization.
- **Topics Covered**
  - Overview of vulnerability scanning
  - Greenbone Community Edition (formerly OpenVAS)
  - Nessus and Nexpose/InsightVM by Rapid7
  - Nuclei vulnerability scanner (YAML templates)
  - **Exercise**: Set up Greenbone (OpenVAS) for a scan, then perform a Nuclei-based assessment

Module 8 – Shells & Payloads

- **Learning Objectives**
  - Differentiate between bind and reverse shells.
  - Craft custom payloads and bypass modern antivirus solutions.
  - Launch web shells for post-exploitation scenarios.
- **Topics Covered**
  - Basics of shell types (bind vs. reverse)
  - Automating payload delivery with Metasploit
  - Custom payloads using MSFVenom
  - Bypassing Microsoft Defender
  - **Web Shells**: Laudanum, Antak**,** Weevely**,** Chopper
  - **Exercise**: Generate stealthy payloads that bypass Microsoft Defender

Module 9 – Metasploit Framework

- **Learning Objectives**
  - Master Metasploit's module structure and workflow.
  - Use encoders, databases, and Meterpreter for advanced attacks.
  - Evade firewalls and IDS/IPS effectively.
- **Topics Covered**
  - Metasploit modules overview
  - Encoders for obfuscation
  - Sessions & job management
  - Meterpreter usage and post-exploitation modules
  - **Exercise**: Obtain a reverse shell, escalate privileges, and maintain access

Module 10 – Exploitation

- **Learning Objectives**
  - Identify vulnerable services and misconfigurations.
  - Exploit various network and service vulnerabilities.
  - Leverage well-known exploits (DNS zone transfers, SMB, FTP, email services).
- **Topics Covered**
  - Common service misconfigurations
  - DNS Exploitation (Zone Transfer Attacks)
  - Email, FTP, SMB exploitation

- SQL attacks
- Password spraying with CrackMapExec **/** Impacket
- **Exercise**: Perform DNS zone transfer attacks; enumerate and exploit SMB shares

Module 11 – Pivoting

- **Learning Objectives**
  - Tunnel traffic through compromised hosts to access isolated networks.
  - Configure port forwarding using SSH, Meterpreter, or other tools.
- **Topics Covered**
  - Overview of pivoting and its purpose
  - Dynamic/Reverse port forwarding with SSH (on Linux & Windows)
  - Meterpreter-based pivoting
  - Chisel and Ncat for pivoting
  - **Exercise**: Configure port forwarding/tunneling and access internal network hosts

Module 12 – Password Attacks

- **Learning Objectives**
  - Capture and crack password hashes on Windows and Linux systems.
  - Use captured hashes for “Pass the Ticket” and lateral movement.
- **Topics Covered**
  - NTLM hash capturing and cracking (Hashcat, JohnTheRipper)
  - SAM, LSASS, NTDS.dit attacks
  - Credential hunting
  - Pass the Ticket (PtT)
  - **Exercise**: Perform PtT attack and lateral movement with captured NTLM hashes

Module 13 – Active Directory Enumeration & Attacks

- **Learning Objectives**
  - Enumerate AD relationships using automated tools (BloodHound, PowerView).
  - Perform Kerberoasting, AS-REP Roasting, and exploit modern AD vulnerabilities.
  - Understand advanced AD attacks (DCSync, trust relationship exploits).
- **Topics Covered**
  - AD roles, components, importance in enterprise security
  - BloodHound & PowerView usage
  - Kerberoasting, AS-REP Roasting
  - Modern AD vulnerabilities: ZeroLogon (2020), PetitPotam, PrintNightmare, DFSCoerce
  - DCSync attacks
  - **Exercise**: Use BloodHound for enumeration and perform a DCSync attack

Module 14 – Post-Exploitation

- **Learning Objectives**
  - Escalate privileges (horizontal/vertical).
  - Establish persistence mechanisms and perform cleanup.
- **Topics Covered**
  - Privilege escalation strategies

- Persistence (scheduled tasks, services, registry)
- Log evasion/cleanup techniques
- **Exercise**: Escalate privileges, set up persistence, and clear event logs

Module 15 – Windows Privilege Escalation

- **Learning Objectives**
  - Exploit dangerous privileges, groups, and service misconfigurations.
  - Demonstrate real-world escalation paths in modern Windows environments.
- **Topics Covered**
  - Abusing SeImpersonate, SeAssignPrimaryToken, SeDebugPrivilege
  - Abusing groups like DNSAdmins, Print Operators (PrintNightmare example)
  - Unquoted service path attacks
  - Legacy but still found in the wild**:** EternalBlue (MS17-010)
  - **Exercise**: Abuse DNSAdmins group, exploit SeBackupPrivilege for escalation

Module 16 – Linux Privilege Escalation

- **Learning Objectives**
  - Enumerate and abuse SUID binaries and sudo misconfigurations.
  - Escape container-like environments (lxd, Docker) if present.
- **Topics Covered**
  - SUID exploitation with GTFOBins
  - Cron job abuses for reverse shells
  - Python library hijacking
  - Dirty Pipe vulnerability (modern kernel exploit)
  - **Exercise**: Break out of the lxd group or Docker container to gain root access

Module 17 – Web Attacks

- **Learning Objectives**
  - Identify and exploit critical web vulnerabilities (XSS, SQLi, RCE, etc.).
  - Apply secure coding awareness to advise on mitigations (OWASP Top 10 2021 / API Top 10 2023).
- **Topics Covered**
  - Cross-Site Scripting (XSS)
  - SQL Injection (SQLi)
  - CSRF, LFI/RFI, IDOR, XXE
  - File upload attacks, path traversal, open redirects
  - Broken authentication and session misconfiguration
  - **Exercise**: Exploit multiple web app vulnerabilities in the online labs

Module 18 – Container & Cloud Security

- **Learning Objectives**
  - Recognize fundamental misconfigurations in Docker/Kubernetes.
  - Identify cloud misconfigurations (AWS IAM, S3 buckets, Azure privileges).
- **Topics Covered**
  - Docker environment enumeration & privilege escalation
  - Kubernetes cluster recon (if time/labs allow)

- Common cloud flaws (exposed storage buckets, overly permissive IAM roles)
- **Exercise**: Access a misconfigured container and escalate privileges; examine a mock cloud environment for vulnerabilities

Module 19 – Reporting

- **Learning Objectives**
  - Document findings clearly for technical and executive audiences.
  - Utilize frameworks and collaborative platforms for continuous reporting.
- **Topics Covered**
  - Dradis Framework basics
  - Executive summaries vs. technical details
  - Evidence collection and presentation (screenshots, logs, POCs)
  - Introduction to Faraday or Serpico for collaborative reporting