

Elite Penetration Testing Training

Top Courses

Web App Testing
&
Infrastructure Testing

Customers

Top Banks,
Financial Services,
Insurance &
Government Clients

Elite Trainers

OSCP Certified
CREST Certified
CHECK Team
Leaders

Black Hat Trainers

Learn from trainers
who teach at
prestigious Black Hat
Events

Why Use Us:

Globally, highly skilled penetration testers are a valuable but rare breed of people. Consequently, organisations are left with no choice but to devote a significant portion of their budgets to external testing service providers.

Cyber Management Alliance Ltd (CMA Ltd) is on a mission to narrow this gap and empower business by:

- Lowering their dependency on external security talent and maximising security budgets
- Providing world class elite training and knowledge to select employees
- Offering bespoke training based on individual business requirements

Course Offerings

- Infrastructure Training – 4days
- Infrastructure Hacking (Intermediate)
- Advanced Infrastructure Class(Advanced)
- Web Application Security – 4days
- Secure Coding Practices – 4days
- Mobile Application Security – 4days

- Infrastructure Training is offered in two classes
- with difference in complexity of challenges and
- advanced topics.





Hands On

Interactive

Advanced

Black Hat
Edition

INFRASTRUCTURE TRAINING - BLACK HAT EDITION

Overview (both intermediate and advanced classes)

This 4 day course will teach you various attack techniques to compromise various operating systems, networks and/or devices. Whatever your final objectives like penetration testing, Red Teaming, or gaining a better understanding of managing vulnerabilities in your environment, understanding advanced hacking techniques for infrastructure devices and systems is critical.

You will be hacking into these challenges and will be compromising domains, systems and/or devices.

Who Should Attend

- Sys admins, SOC staff, security analysts consultants, information security officers, anyone who wants to improve their skill-set.
- This also helps students to prepare for advanced examinations such as Crest CCT exam, Tiger exams, OSCP, etc.

- **Pr-requisites;** Own laptop with VMWare or other similar product
- An understanding of Windows/Linux concepts is necessary and any security knowledge is a bonus.

Four Days Syllabus

Text in **RED** relates to Advanced topics & challenges

Day 1

- TCP/IP Basic Concepts
- Open Source Intelligence (OSINT)
- Network scanning – Probing, The Art of Port Scanning (TCP/UDP/ICMP)
- Service Enumeration Techniques (Windows/Linux)
- Hacking Application Servers
- Brute Force Attacks – Multiple services
- Password Cracking – Tips, Tricks and Challenges

Day 2

- Windows Hacking – Windows vulnerabilities, exploitation using local & remote exploits, **multiple privilege escalation challenges***. **Some of the hacks include** MS14-068 (Kerberos forged tickets), pass the hash, domain compromises.
- Metasploit Crash Course - Exploitation, pass the hash, custom payloads, **anti-virus evasion*** and post-exploitation topics

Day 3

- Assessing Linux services
- Service Enumeration (Finger, SSH, NFS, RPC, etc.)
- Service mis-configurations, and **Linux mis-configurations for privilege escalation***
- Exploitation and Mitigation

Day 4

- Hacking VoIP Solutions
- Attacking VPNs
- **VLAN Hopping (VLAN attacks, traffic sniffing exercises)***
- B33r 101

For further information or to register, call our call centre +44 203 1891422
or email info@cm-alliance.org



Hands On

Interactive

Advanced

Web
Focused

WEB APPLICATION SECURITY TRAINING

Overview (both intermediate and advanced classes)

This three day course on web application security is taught by our expert web app tester who has over 8 years of experience in web app pentesting.

He has been a delivery team lead for all engagements relating to Web Application Testing of Commercial and Retail Customers and has several years of testing mobile applications for Banking / Financial sector clients.

You will also gain experience in testing cloud based technologies and learn how to break in to Android and Apple phones.

Who Should Attend

- Sys admins, SOC staff, security analysts consultants and those with some coding experience and anyone interested in information security

Three Days Syllabus

Day 1 Web Application Basics

- Application architecture
- Web technologies & HTTP basics
- Current attack trend
- Application Security overview
- Common pentest tools overview & Google hacking

Application Test Methodology

- Port scanning & Web server assessment & SSL security
- Default configuration / Common CMS exploitation techniques

Day 2 OWASP Top 10 / Application Vulnerabilities

- Authentication & Authorisation vulnerabilities
- Session management security
- Business logic flaws
- SQL Injection – Blind, Error based, Time, out-of-band
- Cross Site Scripting – DOM, Reflected, Stored
- Insecure direct object references
- Broken Access Control
- Cross-site Request Forgery & Unvalidated redirects and forwards
- Input validation & encoding, File Inclusion – LFI, RFI
- Privilege escalation opportunities & Session Fixation

Day 3 Web Services Assessment

Web services / XML Attacks & Web services overview
XML security & SOAP/ WSDL/JSON/AJAX hacking

Advanced Hacking Techniques
Clickjacking, Flash / Java application security
.Net Remoting & Advanced SQL Injection

Capture the Flag
Challenges & Quiz &
Hack lab access

For further information or to register, call our call centre +44 203 1891422
or email info@cm-alliance.org