



Hong Kong
Fortis Bank Tower
77-79 Gloucester Road
Wanchai
Hong Kong
Ph: +852 8175 2029

Australia
Level 50
120 Collins Street
Victoria Australia
Ph: +61 (0)3 9018 7764

www.kustodian.com

Elite Hacking – Covert Hacking Course :: Official Course Outline

Key Data

Duration:

5 days (60 hours)
Hours: 11am – 11pm

Languages:

– English

Format:

Instructor-led Course (lecture and labs)

Prerequisites:

- Intermediate Level TCP/IP Skills
- Advanced Linux OS Skills
- Advanced Windows OS Skills
- Intermediate Unix Skills
- Intermediate IPS/IDS Skills
- Intermediate Routing Skills
- Intermediate Programming Skills

Student Materials:

1. Student Workbook
2. Student Reference Manual
3. Software/Tools 1 x DVD's

Elite Hacking – ICovert Hacking Course for Advanced Professionals Course Description

You have done all the hacking training out there, CEH, CPTS, Extreme Hacking but where to from here. The Elite hacking course is a course for Advanced Security Professional wanting to take there skills to the highest level. This course is built on real Penetration Testing with IPS evasion, Social Engineering and attacking a 3 tiered banking architecture into the internal LAN environment. The knowledge in this course is built from years of experience working with the military and finance industries around the world. This course is not a 9-5 course; it consists of 12 hour days in a relaxed atmosphere. Students will bring in there own custom built computers/laptops with their attack tools. Students will leverage of the instructor and other students on attack methods and the latest technologies.

The course is graded advanced skill level in TCP/IP, IDS/IPS, Routing, firewall, UNIX and Hacking technology. Students will focus on hands on analysis and attack patterns. This is an intensive 5 day course hands on course.

Kustodian trainers keep abreast of their expertise by undertaking consulting, as we believe that an equal emphasis on theoretical and real world experience is essential for effective knowledge transfer to you, the student. The Elite hacking course is nor a course for the faint hearted, and a high level of skill is required to even sit the class. Instructors are full time penetration testers working with large corporations and the military. The course also enhances TCP/IP skills needed to identify new attack patterns, and techniques for identifying them. The course also shows students attack patterns that can not be detected by IDS/IPS devices and how to defend against them.

Upon Completion

Upon completion, student will have an in-depth knowledge of elite hacking techniques and avoiding detection as well as excellent counter hacking skills. Students will be able to identify attack patterns, source of the attack and how to respond to the threat quickly and effectively. Students will enjoy an in-depth course that is continuously updated to maintain and incorporate the ever changing security environment. This course offers proprietary laboratories that have been researched and developed by leading security professionals from around the world.



Course Module Summary

Module 1 - TCP/IP Packet flow patterns depth analysis

Module 2 - Packet Inspection and Analysis

Module 3 - Hacker attack tools and resulting IDS logs to identify attack tool

Module 4 - Cryptography technology to mask an attack

Module 5 - Evading IDS detection techniques

Module 6 - Social Engineering

Module 7 - Fully compromising a 3 Tiered Architecture through the DMZ without detection

Module 1: TCP/IP Packet flow patterns in-depth analysis

This module is an advanced look at communications at each OSI layer. Hackers use advanced knowledge of TCP/IP, UDP, ARP, IPX and session application layers to not trigger alerts on Intrusion Detection Systems.

- OSI Layers
- Protocol Inspection
- Packet Filters
- Stateful packet inspection
- Protocol standards
- IPS/IDS at each OSI layer

Module 2: Packet Inspection and Analysis

Packet inspection and analysis are the most important requirement for successfully identifying attacks or false positives. This module teaches how to approach log analysis, single packet or packet stream analysis and identifying the attacker in a sea of decoy random packets.

- Packet Inspection Methods
- Bleeding Edge Packet Inspection techniques
- Inline Application layer modification
- Packet size analysis
- Single Packet attack breakdown
- False Positives
- Identifying the attacker and stopping the attack
- Identifying the attacker in a sea of decoy packets
- Sorting through the volumes of logs
- Well known attacks at each OSI Layer

Module 3: Hacker attack tools and resulting IDS logs to identify attack tool

We step into the mind of a Professional Hacker and use every tool and related syntax at our disposal; against the IDS system we have set up in a previous lab. Students will run the hacker tools using SYN, FIN, ACK, XMAS type scans against the IDS system and then analyze logs to see which tool and which syntax was used to cause the corresponding log entry. From these entries students will then piece together the attack, its destination and its source to apply the effective response to the threat.

- Port Scanners (Nmap, Xprobe2, Amap, scanrand) / Analysing IDS logs
- Vulnerability Assessment Tools (Nessus, ATK, Xscan) / Analysing IDS logs
- Automated Penetration Tools (Metasploit, Core Impact) / Analysing IDS logs



- VPN tools (IKE-Scan, IKE-Probe) / Analysing IDS logs
- Brute Force tools (Hydra, Brutus, Munga Bunga) / Analysing IDS logs
- Web Page Attack tools (Nikto, Wikto, Nstealth, Paros) / Analysing IDS logs
- Attack Code in HTTP headers
- SQL Injection, Cross Site Scripting
- Brute Force Browsing
- Polymorphic shell code and IDS bypass through race conditions
- 0 day Exploits

Module 4: Cryptography technology to mask an attack

Cryptography can be used to hide attacks on ports such as 443 and 22 where the IDS can not see into the data stream unless keys are stored on the IDS / IPS device. This module reinforces how cryptography works and how attackers use it to bypass detection. Tools in labs to show the students what tools are being used and how to identify hackers' activity by hiding data in encrypted channels.

- Symmetric Encryption
- Asymmetric Encryption
- Port forwarding using SSH through a DMZ
- IPSEC, SSH
- CryptCat
- Stunnel
- Firewall
- Local Port Binding

Module 5: Evading IDS detection techniques

Security Professionals academics and Hackers are currently developing techniques, tools and skills to bypass Intrusion Detection Systems. Papers are being released weekly in journals and online to share. This module uses hands on labs too see these attacks place. It also shows signature packets which can be used to identify the attacker and the attack being used. Students will play the role of the hacker and security analysts and try to bypass the IDS systems. Each time they run an attack pattern they can view the corresponding logs created (if any) on the IDS system.

- Spoofed Packets
- Malformed Packets
- Encrypted paths
- Decoy Scan
- Fragmented Packets
- Bounce Attacks
- Covert/Overt Attacks
- Timing attacks
- IDS Evasion tools and probes (Fragrouter, Hping2, Packetto)
- Slow port scanning techniques



Module 6: Social Engineering

Corporations with skilled security staff make it difficult to penetrate a company using technical attacks. Social Engineering makes it easy. Simply by doing the reconnaissance it is a matter of simply walking into the office planting key loggers, wireless access points or 'Creep boxes'. We are now on the internal network, and don't have to worry about firewalls. Social engineering is the technique of circumventing technological and physical security measures by manipulating people to disclose crucial authentication information. This module will show the student on how to manipulate the weakest link; people.

- Reconnaissance
- Creating a Wireless Access Point bridge to plant internally
- 'Creep box' – Dial in by GSM and connect after planting internally
- How to read a person
- Reverse Social Engineering
- Mail Spoofing Internal
- Mail Spoofing External
- Social Engineering over the phone
- Social Engineering physical attack
- Hardware key loggers
- What to steal
- Blending into the office

Module 7: Fully compromising a 3 Tiered Architecture

This module is concentrated on for 3 days. The students will get hands on hacking attack of a functioning 3 tiered banking architecture including border facing routers, ISP ASN, Firewalls, IPS, Web Servers and supporting servers, Middleware and Database Servers. Participants can see their attacks at every stage, what the Security Architect/Analyst would see when the attack was taking place and how to remain undetected. Students will perform an attack and the instructor will use LCD screens to show you where they went wrong or what there attack looks like from the other side on a full display. There are no time constraints on this module and students are encouraged to think outside the square.