



**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](http://www.kustodian.com)

# Intrusion Detection- Prevention Analysis :: Official Course Outline

## Key Data

**Course Number:**  
IDS-IPS Analysis

**Duration:**  
5 days

**Languages:**  
– English

**Format:**  
Instructor-led Course (lecture and labs)

**Prerequisites:**  
– Intermediate Level TCP/IP Skills  
– Intermediate Linux OS Skills  
– Intermediate Windows OS Skills  
– Basic Snort IDS Software

**Student Materials:**  
1. Student Workbook  
2. Student Reference Manual  
3. Software/Tools 1 x CD's

## IDS-IPS Analysis- Intusion Dection and Prevention Analysis Course Description

Intrusion Detection and Prevention Systems are used in both in the military and corporate networks around the world to help identify and prevent attacks from taking place at the door of the network or internal to the network. However the complexity of these product leads to many false positives alerts or even worse a true positive than is dismissed because of the complexity or no understanding of the attack used. This course is focused on an in-depth technical analysis of the IDS/IPS logs to identify where the attack is coming from, what sort of attack pattern and how to stop it. It also shows IDS/IPS limitation and shortcomings.

Students will learn how an attacker thinks, what tools a hacker will use and be able to identify which attack tool and syntax the attacker is using. Whether the attack is a simple FIN port scan, decoy scan or a SQL injection string, students will be able to identify the attack patterns and stop the hacker in their tracks.

The IDS-IPS course is graded Intermediate to Advanced skill level in TCP/IP, IDS/IPS 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 IDS-IPS Analysis Course presents information on the latest hacker attack patterns and how to identify these attacks on the IDS system. 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, IDS-IPS student will have an in-depth knowledge of installing, configuring and monitoring Intrusion Detection Systems. 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** - Introduction to Intrusion Detection / Prevention Systems

**Module 2** - Installing and Configuration of Snort on a Secure Linux platform

**Module 3** - TCP/IP Packet flow patterns depth analysis

**Module 4** - Packet Inspection Technology and Analysis

**Module 5** - Hackers methodology

**Module 6** - Hacker attack tools and resulting IDS logs to identify attack tool

**Module 7** - Cryptography technology to mask an attack

**Module 8** - Evading IDS detection techniques

### Module 1: Introduction to Intrusion Detection / Prevention Systems

This module is a brief introduction into Intrusion Detection and Prevention Systems and to discuss their strengths and limitations. It also demonstrates the most effective positioning of these devices in a network infrastructure and common mistakes in architecture designs.

- Network Intrusion Detection Systems
- Intrusion Prevention Systems
- Limitations and Strengths
- Network Architecture
- Defence in Depth principle

### Module 2: Installing and Configuration of Snort on a Secure Linux platform

This module is a hands on lab that demonstrates the correct way in setting up Snort on a Linux Platform. This includes the securing of the server, Operating System, Apache, MySQL /SQL/ OpenSQL, Snort and BASE using United States NSA standards. Great detail is focused on preparing snort configuration files, backups, alerts and rule sets.

- Installing and configuration of Snort
- Securing the Snort/Linux Server including Apache/SQL lockdown (running BASE, ACID)
- Setting the configuration files
- Backing up of logs and databases
- Alerting and filters

### Module 3: 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 4: Packet Inspection Technology 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 5: Hackers methodology

Hackers use a systematic approach when trying to penetrate or trespass a target system whether they are script kiddies or professional Hackers. Script kiddies will try automated tools to bypass a system including hard hitting port scans leaving a heavy footprint on an IDS system. Professional Hackers will be slightly more discreet methodology but they all follow the same attack patterns. This module shows how a hacker works operates on a target and shows the students how to identify not only the attack pattern but the degree of skill they are up against to apply the appropriate response.

- Passive Scanning
- Foot Printing
- Enumeration
- Denial of Service
- Virus and Trojan Behaviour
- Backdoors / Rootkits

## Module 6: 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 7: 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
- IPSEC, SSH
- CryptCat
- Stunnel
- Firewalk
- Local Port Binding

## **Module 8: 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 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