

The Center for Infrastructure Assurance and Security

Introduction to Intrusion Detection Systems

About Us

The CIAS was formally launched in 2001 through a cooperative effort of representatives from industry, government, and academia. We are designed to leverage the Infrastructure Assurance and Security (IAS) strengths resident in San Antonio, Texas as part of the solution to the nation's Homeland Security.

The CIAS has developed a robust set of Security Training courses designed to address security issues from the beginner to the IA professional. These courses are ready for delivery and can be customized to meet an organization's unique cyber security needs. Our instructors are highly qualified and maintain currency in the security field. Our capabilities include an onsite classroom located at the CIAS facility and a mobile classroom available for training at your location.

For more information about the CIAS, please visit our web site:
<http://www.utsa.edu/cias>

Contact

Jenine Stevenson
Program Coordinator
210.458.2185
210.632.6597
Jenine.Stevenson@utsa.edu

Overview

This 5-day lecture and hands-on training course provides an introduction to the theory, technology, and implementation of intrusion detection/prevention systems. Lecture material covers the range of intrusion detection issues, while the practical exercises reinforce the lectures and allow students to implement an intrusion detection system. Students attending this course receive a Certificate of Completion.

Audience

Professionals working in system, security, and network administration or engineering who need to fill gaps in their understanding or are new to intrusion detection systems should attend.

Prerequisites

Computer literacy is required. Students should be familiar with a windowed Graphical User Interface (GUI) computing environment. Some knowledge of networking and TCP/IP is beneficial.

Course Materials

Lectures, practical exercises, and reference materials are provided.

Course Contents

- TCP/IP
- Packet Analysis
- History of Intrusion Detection Systems
- Host-based IDS
- Network Based IDS
- Networks and NIDS Placement
- IDS Signatures & Operations
- Deploying an IDS
- IDS vs. IPS
- Tuning
- Analyzing IDS Data
- Common IDS Alarms
- Reports and Reporting Tools
- Procedures
- IDS Evasion Techniques
- Other Applicable Topics

