

# OSCS-2 - INTRUSION DETECTION & PREVENTION SYSTEMS

Categoria: **Cyber Security**

## INFORMAZIONI SUL CORSO



**Durata:**  
3 Giorni



**Categoria:**  
Cyber Security



**Qualifica Istruttore:**  
Docente Senior (min.  
5 anni)



**Dedicato a:**  
Professionista IT



**Produttore:**  
PCSNET

## OBIETTIVI

Questo corso presenta le tecniche di Intrusion Detection and Prevention Systems (IDPS) ed è indirizzato ai tecnici che operano e gestiscono la Sicurezza delle Reti

## PREREQUISITI

Buone conoscenze sistemistiche e di reti

## CONTENUTI

### **Architettura di un Intrusion Detection and Prevention System (IDPS)**

- Generalità
- Principi di intrusion detection e prevention
- Metodi di intrusion detection
- Signature-Based Detection
- Anomaly-Based Detection
- Stateful Protocol Analysis
- Componenti e architettura
- Funzioni di sicurezza
- Implementazione e amministrazione dell'IDPS
- Tipi di tecniche di IDPS
- Network-Based IDPS
- Wireless IDPS
- Network Behavior Analysis (NBA) System
- Host-Based IDPS
- Integrazione di molteplici tecniche IDPS
- Scelta dei prodotti IDPS

### **Shell Testuali e IDPS**

- Introduzione
- Le shell
- Shell Testuali

- Shell Grafiche
- Vulnerabilità nelle shell testuali
- Il dataset di Schonlau

### **Panoramica di Tecniche di Intrusion Detection in shell testuali**

- Introduzione
- I risultati delle varie Tecniche
- Presentazione delle Tecniche
- Layered Networks based on ECM e Support Vector Machine based on Co-occurrence Matrix
- RBF Neural Network
- Sequence Alignment
- Naive Bayes
- Recursive Data Mining
- Uniqueness
- Bayes one-step Markov
- Hybrid Multi-step Markov
- Compression
- IPAM – Incremental Probabilistic Action Modeling
- Sequence Matching

### **INFO**

**Materiale didattico:** Materiale didattico e relativo prezzo da concordare

**Costo materiale didattico:** NON incluso nel prezzo del corso

**Natura del corso:** Teorico Metodologico