OSS Security Training Plan

Server Security

Objectives

To protect the server and data from intentional and non-intentional attacks

Prerequisites

Experience in System administration
Experience or some knowledge in setting Database server
Basic networking skill

Training Outcomes

At the end of the courses the students should be able to perform the following:

One Day Course:

- O/S level security

Three Days Course:

- O/S level security
- Application level security

Ten Days Course:

- O/S level security
- Application level security
- Database level security
- Intrusion Detection

Laboratory requirements

The lab should be able to provide hands-on training for the participants. The labs should also be able to support one, three or ten days courses.

Hardware
Servers (minimum 2 units for possible clustering)
Terminals (individual participant)

Software
O/S (that can support clustering)

Network
Wired and Wireless LAN in its own separate segment

One Day Course

Basic O/S related security

- Introduction to Linux Security Model
- Partitioning and File System Security
- Configure Security, Authentication and Access Settings
- Apply Security Updates
- Log Concept
- Understand Services and Protocols
- Introduction to secure remote administration
- Understand Firewall
- Simulated Attack

Three Day Course

The first day would be ***"Basic O/S related security"*** (refer to above). The second and third day would cover:

- Managing Permissions
- Finding unsecured files
- Packet filtering
- IPTables
- Cryptography Basics
- SSL and VPN
- Securing Remote Access into the server
- Securing Apache with SSL
- Application-Level Gateway Basics
- Configure and Use of Proxy
- The Basic of Securing Services
- Audit and Log

Ten Day Course

The first three days would cover the topics in the three day course. The other topics related to:

- Database level security
- Intrusion Detection

Will be covered in detail

- Introduction to Ethical Hacking
- Analysing your server security (e.g.: detecting/preventing Trojans, backdoors, bruteforce attack)
- DDoS attack
- IDS and IPS