ANI CONSUMER SOLUTIONS PRIVATE LIMITED
CIN: U74999DL2016PTC308530
Phone: +91-9711212660 Email: aniconsumersolutions@gmail.com
Website: http://aniconsumersolutions.com/

"Perimeter Security from Cyber Attacks"

Duration: 2 Days

Eligibility: B.Tech/BE & MBA Students

Training Objective: Ensure the confidentiality, integrity, and availability of your organization's information by protecting your communications and data. In this training course, you learn how to define and implement security principles, install and customize secure firewalls, build Virtual Private Network (VPN) tunnels, and safeguard your organization's network perimeter against malicious attacks.

Course Contents:

- **Defining security principles**
  Ensuring data Confidentiality, Integrity and Availability (CIA)
  Assessing defensive techniques
  Setting a generic security stance

- **Developing a security policy**
  Balancing risk with business requirements
  Identifying your information assurance objectives
  Choosing security technologies

- **Deploying a Secure Firewall**

- **Installing a firewall**
  Determining the appropriate firewall type
  Selecting and hardening the operating system
  Virtualizing the firewall appliance

- **Configuring a firewall to support outgoing services**
  Supporting simple services: HTTP, SMTP
  Filtering dangerous content and handling encrypted traffic
  Managing complex services: VoIP, audio and video

- **Providing external services securely**

Implementing publicly accessible servers
Building a DMZ architecture
Supporting SMTP mail

- **Allowing access to internal services**
  Customizing DNS for firewall architectures
  Configuring Network Address Translation (NAT)
  Developing access lists for client server applications

- **Detecting and Preventing Intrusion**

- **Deploying an IDS**
  Placing Network IDS (NIDS) within your network architecture
  Operating sensors in stealth mode

- **Detecting intrusions in the enterprise**
  Designing a multi-layer IDS hierarchy
  Managing distributed IDS

- **Interpreting alerts**
  Verifying IDS operation
  Minimizing false positives and negatives
  Validating IDS events and recognizing attacks

- **Stopping intruders**
  Exploiting IDS active responses
  Snipping a TCP session
  Controlling access with a firewall update

- **Configuring Remote User Virtual Private Networks (VPNs)**

- **Building VPN tunnels**
  Compulsory vs. voluntary tunnels
  Supporting remote users with layer 2 tunnels
  Connecting remote sites with layer 3 tunnels

- **Deploying client software**

Assessing remote access VPN alternatives
Implementing remote user authentication
Leveraging Layer 2 Tunneling Protocol (L2TP)
Protecting L2TP tunnels with IPsec Transport Mode

- **Creating Site-to-Site VPNs**

- **Applying cryptographic protection**
  Ensuring confidentiality with symmetric encryption
  Exchanging symmetric keys with asymmetric encryption
  Checking message integrity with hashing
  Managing digital certificates with PKI

- **Comparing tunneling and protection methods**
  Employing VPN concentrators and VPN-capable routers
  Applying IPsec Tunnel Mode
  Assessing tunneling protocols
  Evaluating VPN topologies

- **Integrating Perimeter Defenses**

- **Reducing the impact of denial-of-service (DoS) attacks**
  Mitigating bombardment attacks
  Rejecting connection-based attacks with IPSs
  Blackholing and sinkholing
  Implementing a DoS Defense System (DDS)
  Blacklisting attack sites and address ranges

- **Perimeter architectures**
  Integrating IDS and VPNs with your firewall architecture
  Positioning externally accessible servers
  Monitoring and controlling wireless networks

Note: Learn from SME's; acquire deep insight of subject by learning from subject matter experts of perimeter security technologies.