KOENIG
step forward

Snort Course Content

1. Introduction of Network Design

- Introduction of components of security and CIA Triad
- Introduction of Network Threats
- Common Terminology and Attack
- Hacking Phases , and introduction
- Firewall, and Types of Firewall
- DMZ delimitation and design
- IDS Definition and design
- IPS Definition and design
- Introduction to Iptables

2. Modes of Snort

- Introduction of NIDS, NIPS , HIDS
- Different logging mode of snort
- Features of Snort
- Introduction of DAQ and modes of DAQ
- Understanding Basic Output of Snort
- Inline mode
- Passive Mode

3. Snort Installation

- Installing Snort IDS in Windows Environment
- Installing Snort in Linux Environment ,
- Installing Snort IPS to work with iptables
- Snort Configuration File
- Different Configuration Options in Snort.conf

4. Basic Rule Writing of Snort

- Structure of Snort Rules
- Component of Snort Rule
- Rule Options of Snort
- General Rule Options
- payload Rule Options
- Non Payload Rule options

- IPS Rules Action ,

5. Lab Implementation of Snort IDS , Log and Alert Analysis

- Installation and configuration of Snort IDS
- Testing IDS deployment by simulating attack

6. Lab Implementation of Snort IPS , and Blocking Traffic

- Installation and configuration of Snort IPS
- Testing IPS deployment by simulating attack.