

## **Course Description**

Course helps students or professionals to kick start their career in Linux.

## **Course Benefits**

Few of the key benefits to opt this course are:

- 1) Kickstarts your career in Linux Technology
- 2) Increased understanding about operating system and networking concepts
- 3) Demonstrate your competence to a potential employer

## **Post-Training Benefits**

Company provides following benefits to the students undergoing this course:

- 1) Association with large Linux Community
- 2) Assistance in Summer Internship
- 3) Job Placement Assistance

## **Target Audience**

Students, Windows Administrators, Desktop Engineers, Software Developers and other professionals interested in learning Linux.

## **Mandatory Pre-requisites**

Operating system concepts and basic commands

## **Helpful Pre-requisites**

Computer Background

## **Course Duration**

48hrs

<b>1</b>	<b>Introduction to Linux</b>
1.1	Objective
1.2	History and evolution
1.3	UNIX war and most popular flavours
1.4	UNIX overview
1.4.1	Kernel
1.4.2	File system
1.4.3	Devices and directories
1.4.4	Process management
1.4.5	Directory structure
1.4.6	UNIX shell
1.4.7	Quick help (man)
<b>2</b>	<b>Getting Started</b>
2.1	Installation
2.1.1	Analysis
2.1.2	Installation media
2.1.3	Installation modes (graphical, text)
2.1.4	Disk partitioning (RAID, LVM, auto-partitioning)
2.1.5	Disk naming convention
2.1.6	Package selection
2.1.7	First login
2.2	User environment
2.2.1	Environment variables
2.2.2	PATH variable
2.2.3	Command aliases
2.2.4	Commands history
2.2.5	Switching consoles
2.3	Booting Process
2.3.1	Booting sequence
2.3.2	Boot loader
2.3.3	Run-levels
<b>3</b>	<b>System Administration</b>
3.1	Working with Directories
3.2	Working with Files
3.2.1	Command line shortcuts
3.2.2	Permissions
3.3	File Compression
3.3.1	Introduction
3.3.2	Tar
3.3.3	Gzip
3.3.4	Zip
3.3.5	Additional compression commands

3.4	'vi' editor
3.4.1	Introduction
3.4.2	vi modes
3.4.3	Input commands
3.4.4	Delete, Search and replace commands
3.4.5	Advanced commands
3.5	Redirection and pipe
3.6	Searching techniques
3.7	Important system files and their purpose
3.8	User Management
3.8.1	The /etc/passwd file
3.8.2	The /etc/shadow file
3.8.3	The /etc/group file
3.8.4	Group add command
3.8.5	Group del command
3.8.6	Groupmod command
3.8.7	Useradd command
3.8.8	Userdel command
3.8.9	Usermod command
3.8.10	GUI tools
3.8.11	Super user and sudoers
3.9	Process Management
3.9.1	Introduction
3.9.2	Process listing
3.9.3	Starting process
3.9.4	Stopping process
3.9.5	Analyse resource consumption – top
3.10	Disk Management
3.11	Basic shell scripting
3.12	Scheduling Tasks
3.13	Printer Management
3.14	Software Management
3.14.1	Using RPM
3.14.2	Listing packages
3.14.3	Finding packages
3.14.4	Verifying packages
3.14.5	Updating packages
3.14.6	Removing packages
3.14.7	Additional RPM Features
3.14.8	Redhat Network
3.14.9	Using Yum
3.14.10	Configuring RPM repositories
3.14.11	Compiling Software from source code
3.15	CHROOT

3.16 Understanding Syslog and improving troubleshooting skills

## **4 Network Management**

- 4.1 TCP/IP concepts
- 4.2 IP addressing schemes
- 4.3 Routing concepts
- 4.4 Basic concepts of DNS
- 4.5 Configuring network settings
- 4.6 What are ports and services
- 4.7 Checking for open ports on the system
- 4.8 Testing network, ports and services
- 4.9 Managing services
- 4.10 Remote management (SSH, Telnet, Webmin)
- 4.11 DHCP concepts and configuring DHCP server

## **5 Server Management (Basic Configuration)**

- 5.1 File Sharing
  - 5.1.1 FTP
  - 5.1.2 NFS
  - 5.1.3 Samba
- 5.2 Web Server
  - 5.2.1 Apache
- 5.3 Authentication Server
  - 5.3.1 LDAP
  - 5.3.2 Samba PDC
  - 5.3.3 Kerberos and Active Directory
- 5.4 Domain Name Server
  - 5.4.1 DNS Concepts
  - 5.4.2 Bind
- 5.5 Mailing Solutions
  - 5.5.1 Mailing concepts (SMTP, POP3, IMAP)
  - 5.5.2 Sendmail
  - 5.5.3 Postfix
- 5.6 Proxy Server
  - 5.6.1 Squid

## **6 Linux Security**

- 6.1 Linux OS Hardening
  - 6.1.1 Why to Harden Linux?
  - 6.1.2 Hardening best practices
  - 6.1.3 Hardening necessary services
- 6.2 Sniffing
  - 6.2.1 What is sniffing?
  - 6.2.2 Understanding TCPDump and Ethereal

- 6.3 Firewalls
- 6.3.1 Concepts (Filtering, NAT, Port redirection)
- 6.3.2 Iptables, Shorewall firewall
- 6.4 Port Scanning Techniques
- 6.4.1 Why to Port Scan?
- 6.4.2 Understanding NMAP and various switches

## **7 Introduction to useful tools**

- 7.1 Traffic Monitoring – NMAP
- 7.2 Network Monitoring – Nagios
- 7.3 Clustering – Heartbeat
- 7.4 Reporting – Awstats

## **8 Troubleshooting best practices**

## **9 Troubleshooting assignments**