CISS (certified information security specialist)

This course is designed for individuals who are willing to mould their career in information Security Domain.

This course divides into 5 phases.

First phase contains different servers using regularly in production environment of an organization, Configure & Deploy servers in Windows or Linux infrastructure, Day by day reporting & auditing of servers, Patch Management, Troubleshooting regular issues, Upgrading operating systems, Hardening Servers , Designing & implementing Security policies.

Second phase covers in-depth topic of Networks & different network technologies such as Wan connectivity here we discuss Wan protocols, Network mediators, Media, Configuring Wan connectivity using Routers, Configuring Routing protocols, Implementing Access control lists, Designing Router level & Switch level security implementations, VLAN configurations, Inter VLAN connectivity, Trunking configurations, Troubleshooting network devices.

Third phase completely discuss about Hackers & Hacking Methodologies, different security testing methodologies, how hackers perform network scans, Exploitation, Social engineering attacks, Man in the middle attacks, Web site defacements, password hacking, hiding identity, Deleting evidences, keyloggers, Trojans, Backdooring techniques & dangerous Denial of service attacks and Distributed denial of service attacks, and different counter measures have to be taken care by ethical hackers & identifying security loop-holes by running vulnerability assessments, configure honeypots to trap hackers.

Fourth phase corely concentrates on Investigating hacking incidents, Cyber crime Mechanism, Cyber pornography, Threat mail analysis, Sexual harassment cases, Internet misusage. This phase also discuss Log Analysis, Incidence response, Network forensics, packet analysis & cyber laws.

Final module demonstrates configuration of an enterprise firewall to defend an organization against today's emerging threats, Building a firewall, Configuring policies, Natting, Antivirus & antispam solutions, Integrating firewalls with authentication servers, Implementing Intrusion detection & Intrusion prevention systems, Configuring secure VPN tunnels between multiple branches, testing periodically existing infrastructures security measurements, Updating firewall rules.

Microsoft Certified Solution Expert

Introduction to Microsoft Operating systems
- Introduction to windows server 2008
- What's new in windows 2008 server
- Flavours of windows 2008 server
- Prerequisites to install windows server 2008

Installing Active directory services

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Configuring Windows 7 clients
- Configuring Member servers
- Configure Active Directory Rights Management Service (AD RMS).
- Configure the read-only domain controller (RODC).
- Configure Active Directory Federation Services (AD FSv2).

Creating and maintaining Active Directory objects
- Configuring user & group accounts
- Managing User & group accounts
- Automate creation of Active Directory accounts.
- Maintain Active Directory accounts.
- Create and apply Group Policy objects (GPOs).
- Configure GPO templates.
- Deploy and manage software by using GPOs.
- Configure account policies.
- Configure audit policy by using GPOs.
- Configuring volume shadow copies
- Encrypted file system

Maintaining the Active Directory environment
- Configure backup and recovery.
- Perform offline maintenance.
- Monitor Active Directory.

Configuring Domain Name System (DNS) for Active Directory
- Configure zones.
- Configure DNS server settings.
- Configure zone transfers and replication.
- Configure DNS zones.
- Configure DNS records.
- Configure DNS replication.
- Configure name resolution for client computers.

Configuring the Active Directory infrastructure
- Configure a forest or a domain.
- Configure trusts.
- Configure sites.
- Configure Active Directory replication.
- Configure the global catalog.
- Configure operations masters.

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewalllearning.com, hr@firewalllearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewalllearning.com

Configuring Active directory Roles
- Configuring ADC
- FSMO roles
- Transfer of roles
- Seizing of roles
- RSOP

Install Active Directory Certificate Services.
- Configure CA server settings.
- Manage certificate templates.
- Manage enrollments.
- Manage certificate revocations.

Configuring File and Print Services
- Configure a file server.
- Configure Distributed File System (DFS).
- Configure backup and restore.
- Manage file server resources.
- Configure and monitor print services.

Configuring Remote Desktop Services
- Configure RemoteApp and Remote Desktop Web Access.
- Configure Remote Desktop Gateway (RD Gateway).
- Configure Remote Desktop Connection Broker.
- Configure and monitor Remote Desktop resources.
- Configure Remote Desktop licensing.
- Configure Remote Desktop Session Host.

Configuring a Web Services Infrastructure
- Configure Web applications.
- Manage Web sites.
- Configure a File Transfer Protocol (FTP) server.
- Configure Simple Mail Transfer Protocol (SMTP).
- Manage the Web Server (IIS) role.
- Configure SSL security.
- Configure Web site authentication and permissions.
- Configuring Network Application Services
- Manage the Streaming Media Services role.
- Configure SharePoint Foundation options

Windows Server 2008 Network Infrastructure, Configuring.

- Configuring Addressing and Services
- Configure IPv4 and IPv6 addressing.
- Configure Dynamic Host Configuration Protocol (DHCP).
- Configure routing.
- Configure Windows Firewall with Advanced Security.

Configuring Network Access
- Configure remote access.
- Configure Network Access Protection (NAP).
- Configure Direct Access.
- Configure Network Policy Server (NPS).

Virtual Private Network
- Introduction to VPN terminology
- Remote Access VPN
- Site-to-site VPN
- Configuring PPTP vpn
- Configuring VPN access
- Configuring IPSEC VPN

Monitoring and Managing a Network Infrastructure
- Configure Windows Server Update Services (WSUS) server settings.
- Configure performance monitoring.
- Configure event logs.
- Gather network data.

Applications Infrastructure, Configuring, Deploying Servers
- Deploy images by using Windows Deployment Services.
- Configure Microsoft Windows activation.
- Configure Windows Server Hyper-V and virtual machines.
- Configure high availability.
- Configure storage.

Securing Active directory Environment
- Introduction to firewall
- Types of firewalls
- Differences between client side firewall & Enterprise firewall
- Prerequisites for deploying Microsoft ISA server
- Installing Microsoft ISA server 2006
- Configuring firewall client
- Configuring ISA as a proxy

- URL filtering using ISA
- Configuring remote access VPN using ISA
- Configuring Site-to-site vpn using ISA
- Designing Security Templates
- Deploying Security templates

Security Assesment
- Testing Microsoft networks
- Preparing Audit checklist
- Hardening Microsoft servers

RedHat Enterprise Linux

Introduction to Linux Operating System
- History & Architecture of Linux
- Features of Linux
- File system Hirerachy
- Understand Linux file system hierarchy and pathnames

Install Linux graphically

- Install Red Hat Enterprise Linux and configure the system with firstboot
- Text based installation
- Customizing packages
- Post installation of RHEL 6
- Network Based Installation

Get started with bash

- Understand basic shell concepts,
- Execute simple commands
- Creating, Renaming, Moving & Deleting files & Directories
- VI-Editor
- Use regular expressions to search patterns in files and output; redirect and pipe output
- Basic File permissions
- Use man and info pages and find documentation in /usr/share/doc
- Understand Linux file system hierarchy and pathnames
- manage files from the command line.
- Use hard links, archives and compression

Get started with the GNOME graphical desktop

- Manage files graphically and access remote systems with Nautilus
- Configure the date and time, and configure a printer

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Understand basic disk concepts and manage system disks

Administer users and groups

- Creating & Modifying User accounts
- Managing Mailboz, Home directories
- Configuring Secondary groups
- Password policy Management
- Account Lockout policies
- Granting file permissions
- SUID, SGID, Sticky bit

- Manage group memberships, file permissions, and access control lists (ACLs).

Manage physical storage

- Understand basic disk concepts and manage system disks
- Manage file system attributes and swap space
- Create and format simple partitions
- Creating swap partitions, and encrypt partitions.
- Configuring Raid
- Verifying Redundancy

Managing flexible storage with the Logical Volume Manager

- Understand logical volume concepts and manage logical volumes
- Configuring LVM
- Resizing LVM
- LVM Snapshot Management

Centralized and secure storage

- Access centralized storage (iSCSI) and encrypt file systems.
- Configuring iSCSi targets.

Backup & Recovery

- Types of backups
- Backup using tar
- Backup using cpio
- Disk backup using dump
- Restoring backup data

Managing processes

- Identify and terminate processes
- change the priority of a process

- using cron and at to schedule processes.

Monitor system resources

- Manage CPU, memory, and disk utilization
- Network usage
- Performance monitoring

Tuning and maintaining the kernel

- List, load, and remove modules; use kernel arguments

Installing and managing software

- Introduction to RPM
- Installing, Updating & removing packages using RPM
- Introduction to YUM
- Manage software and query information with yum
- Confguring YUM server
- configure client-side yum repository files

Administer remote systems

- Share and connect to a desktop
- Use SSH and rsync
- configure SSH and remote desktops.
- Control graphical access using VNCVIEWER

Configuring Print service

- Installing Printer modules
- Managing printer using CUPS
- Configuring printer accesible through network

Enhance user security

- grant privileges to users via sudo.

- Configure delegation control

Establish network connectivity

- Understand basic network concepts
- Configure, manage & test network settings
- Configuring system as a router
- Troubleshoot network issues.

Automated installations of Red Hat Enterprise Linux

- Configure kickstart server
- Create and manage Kickstart configuration files
- Client side configuration
- perform installations using Kickstart

Accessing network file-sharing services
- Configuring NFS server
- Assigning permissions for a share folder
- Client side configuration
- Configuring autofs
- Troubleshooting NFS server
- NFS Security
- Configure ftp server
- Deploying ftp server
- Deploying home directories using FTP
- Configuring FTP Banners
- FTP Security

Linux Integration with Windows
- Installing & configuring Samba server
- Configure file and print sharing between windows hosts with CIFS
- Configuring winbind service
- Adding Linux users into windows Active directory
- Configuring samba swat

Remote login Services
- Installing Xinetd services
- Configuring Telnet server
- User/computer based restrictions
- Configuring XDMCP server for Thinclients

Domain Naming Services
- Understanding DNS Architecture
- Configuring DNS servers
- Configuring SOA, MX, CNAME records
- Configuring Slave DNS
- Master-Slave replication configuration
- Configuring caching name service

DHCP MANAGEMENT
- Brief introduction of DORA process
- Configuring DHCP server
- Assigning Dynamic pool
- Mac to IP binding

Web Services

- Introduction to web server Architecture
- Installing & configuring Apache server
- Virtual Ip based webhosting
- Virtual port based webhosting
- Virtual hostname based webhosting

Advanced Web services
- Configuring Authenticated websites
- Permitting/restricting access to users & Computers
- Understand SSL certificates
- Deploying an SSL certificate to a web server
- Installing & Configruing Squid server
- Configuring squid proxy to share internet
- Configuring squid as a firewall
- URL filtering using squid
- Content filtering using squid
- Extension based blocking

SMTP Service
- Introduction to Mail server Architecture
- Configuring sendmail as MTA
- Configuring dovecot as MDA
- Deploying mailboxes for users
- Mail redirection
- Configuring squirellmail

Centralized Authentication using LDAP
- Overview of LDAP
- Configuring openldap server
- Configuring Network user accounts
- Client side configuration
- Configuring NIS server
- Integrating NIS with NFS
- Sharing NIS user Home directories using NFS
- Client side configuration
- Troubleshooting NIS & LDAP

OpenSSH
- Configuring SSH server
- Generating Key pair
- User/group based Restrictions

Analyzing and storing logs

- Configuring Syslog server
- Redirecting client logs to syslog server
- Using 3rd party tools for log analysis (SIEM)

Linux Security
- Brief introduction to FILTER/NAT/MANGLE tables.
- Configuring Iptables
- Network Address Translation
- Configuring Static & dynamic NAT
- Configuring firewall Policies
- URL FILTERING
- Word based restrictions
- Port Redirection
- Configuring User define chains
- Configuring TCP wrappers
- Configuring pam.d

Virtual Private Network
- Introduction to vpn
- Remote accessvpn vs site-to-site vpn
- Configuring Site-to-site vpn

HOST BASED INTRUSION DETECTION SYSTEM
- Installation of tripwire
- Updating tripwire policies
- Verifying File integration with Tripwire
- Troubleshooting IDS

Troubleshooting & Debugging
- Root password Recovery
- Understanding boot process
- Understand runlevels and manage GRUB

Cisco Certified Network Associate (Routing & Switching)

Introduction to Networking
- OSI Model
- Networking Fundamentals and Networking Media

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Components of a LAN
- Cabling LANs and WANs
- Ethernet Fundamentals

IPADDRESSING
- TCP/IP Protocol Suite
- IPv4 Address Classes
- Addressing Fundamentals

IPV4 SERVICES
- Domain Name System
- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Differences between TCP & UDP

SUBNETTING
- Classful vs. Classless Addressing
- Subnet Calculation Process
- VLSM
- CIDR
- Summarization

ROUTER
- Introduction to Router
- Configuring a Router
- Managing Cisco IOS Software
- IOS backup & Recovery
- Password Recovery of router

ROUTING BASICS
- Introduction to Routing Protocols
- Static Routing
- Default Routing
- Dynamic Routing

IP ROUTING PRINCIPLES
- IP Routing Fundamentals
- Link State Protocol
- Administrative Distance

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

ROUTING PROTOCOLS
- IGRP
- Differences between RIPv1 & RIPv2
- Configuring RIP

OSPF
- OSPF Fundamentals
- Configuring OSPF
- OSPF Route Selection
- OSPF Route Preferences

EIGRP
- EIGRP Fundamentals
- Configuring EIGRP
- EIGRP Route Selection
- EIGRP Troubleshooting

Access Control Lists (ACLs)
- Access-List Fundamentals
- Configuring ACL
- Access-List Processing
- Wildcard Masks
- Standard IP Access-Lists
- Extended IP Access-Lists
- Troubleshooting Access-Lists

NETWORK ADDRESS TRANSLATION (NAT)
- Introduction to NAT
- NAT Fundamentals
- Configuring static NAT
- Configuring Dynamic NAT
- NAT Troubleshooting

Port Address Translation
- Introduction to PAT
- Configuring PAT

FRAME RELAY
- Frame-Relay Fundamentals
- Implementing Frame-Relay
- Frame-Relay with ARP

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Frame-Relay Serial Interface

SWITCHING
- Introduction to Switching
- Switch Architecture
- Configuring Cisco switches
- Running debug commands

VLANS
- Introduction to VLAN Technology
- VLAN Principles
- Creating VLANs
- VLAN Trunking
- Configuring Inter-VLAN Routing

Spanning-Tree protocol
- Spanning-Tree Basics
- Configuring Spanning-tree
- Spanning-Tree Convergence
- Spanning-Tree Enhancements
- Spanning-Tree Troubleshooting

Introduction to IPV6
- IPv6 Fundamentals
- IPv6 Routing
- Configuring EIGRP for IPv6
- Completing IPv6 Configuration

WLAN Technology
- Wireless Fundamentals
- Wireless LAN Components
- Wireless LAN Types
- Wireless LAN Operation
- Wireless LAN Security
- Configuring wireless router

Security Device Manager (SDM)
- Introduction to SDM
- Prerequisites of SDM
- Configuring SDM
- Troubleshooting SDM

Cisco Certified Network Associate (Security)

Fundamentals of Security

- Introduction to CIA
- Goals of Security
- Profiles of Attackers
- Types of Attackers
- Typical Threats/Attacks

Security Device Manager (SDM)

- Introduction to SDM
- Prerequisites of SDM
- Configuring SDM
- Troubleshooting SDM

Cisco Device Security

- Configuring SSH server
- Configuring Syslog Server
- Configuring NTP server
- Role based access

AAA (Authentication, Authorization & Accounting)

- Understanding AAA Framework
- Implement AAA on Cisco routers using
- Understanding TACACS+
- Configuring TACACS+
- Configuring Cisco Secure ACS

CISCO Router Based Firewalls

- Classic IOS Firewall
- Drawbacks of CBAC
- CBAC Configuration
- Configuring Zone Based Firewalls
- Implement the Cisco IOS firewall feature set using SDM

Access control Lists

- Access-List Basics
- Exploring Access-Lists
- Applying standard Access /lists
- Extended ACL configuration

Intrusion Detection & Prevention
- IDS/IPS Fundamentals
- Threat Detection Techniques
- Configuring IOS based IPS

Virtual Private Network
- Introduction to VPN
- Types of VPNs
- Internet Key Exchange
- IPSEC Fundamentals
- Configuring Router based Remote Access VPN
- Configuring Site-to-site VPN

Hardening Router
- Running Vulnerability assessment of a router
- Auditing cisco router using SDM
- Configuring one step Lockdown
- Implement secure network management and reporting

Switch Security
- VLAN Attack and Defense
- Spoofing Attacks
- MAC Flooding/CAM Overflow
- STP Attack and Defense
- Configuring BPDU Guard
- Configuring Root Guard
- Overview of Storm control
- Configuring Storm control

Checkpoint Certified Security Administrator

Introduction to Checkpoint Technologies
- What's new in checkpoint R75
- Checkpoint's Architecture
- Implementing 3 tier Architecture of checkpoint

Deployment Platforms
- Checkpoint supported platforms
- Installing Checkpoint on Windows o/s

- Installing Checkpoint on Linux o/s
- Installing Checkpoint on SPLAT
- Configuring checkpoint in standard setup
- Configuring checkpoint in distributed setup
- **Introduction to Security policy**
- Understanding Checkpoint Licensing
- VerifySIC establishment between the Security Management Server and the Gateway using Smart Dashboard
- Creating a basic Rulebase
- Implicit rules vs Explicit rules
- Configuring hide NAT
- Configuring Static NAT

User management & Authentication

- Configure user & group accounts in checkpoint
- Configure policies for authentication
- Local Authentication Methods
- Configuring user authentication
- Configuring Session authentication
- Configuring Client Authentication

External Authentication

- Creating LDAP & TACACS+ objects
- Integrating active directory server with checkpoint gateway
- Configuring Tacacs+ server
- Integrating Tacacs+ server with checkpoint gateway

Identity Awareness

- Introduction to Identity Awareness
- Configuring Identity Awareness
- Using Identity awareness to provide access to network resource

Checkpoint VPN Introduction

- Understanding VPN terminology
- Configuring Remote access vpn
- Implementing site-to-site vpn with head office & Branch office

Monitoring

- Using smartview tracker for Analyzing logs
- Using smartview Monitor for monitoring traffic
- Using queries in smartview tracker
- Filtering logs in smartview tracker

Checkpoint Certified Security Expert

Advance Firewall
- Debugging firewall Modules
- Upgrade & troubleshoot Management server
- Performing Backup of Management server
- Backup using snapshot
- Backup using cpbackup
- Backup using upgrade tools

Command Line Administration
- Understanding standard mode & Expert mode shells
- Running Checkpoint commands
- Accessing Firewall Directory

UTM Features
- Configuring Antivirus blade in checkpoint gateway
- Verifying Antivirus modules
- Implementing content filtering
- Configuring cvp & ufp policies
- Configuring URL filtering
- Testing URL filtering

Advance UTM Features
- Java & ActiveX based attacks
- Implementing Java & activeX blocking
- Configuring Application control
- Using smart event intro for analyzing application traffic

IDS/IPS
- Configuring IPS blade
- Updating IPS signatures
- Configuring IPS policies
- Customizing IPS profiles
- Implementing location based restrictions
- Verifying IPS

QOS
- Understanding Checkpoint QOS architecture
- Enabling QOS blade

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Bandwidth Monitoring using QOS
- Segregate Bandwidth to different networks
- Writing QOS policies in rulebase

CLUSTERING
- Building clusterXL for loadbalancing
- Adding gateways into cluster
- Verify Load balancing
- Bulding clusterXL for High Availabilty
- Deploying HA on an Enterprise network
- Verifying HA using smartview monitor
- Management sever Clustering
- Management server recovery

Web Application Security

Introduction To Web Application
- Introduction to Web Application
- Types Of Web Application
- Use Of Web Application
- Advantage And Disadvantage Of Web Application
- Design Your First Web Application
- Common Attacks On Web Application

Introduction To Database
- Introduction to Database
- Different Types Of Database
- Use Of Database
- Advantages and Disadvantages of Database
- Connecting Database With Web Application
- Common Attacks On Database

Basics Of Web Application Programming
- HTML
- JavaScript
- PHP
- SQL

OWASP Top 10
- SQL Injection

- Cross Site Scripting
- Broken Authentication & Session Management
- Insecure direct Object References
- Cross Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

Implementation of OWASP on DVWA,WEBGOAT
- Overview of DVWA
- Installation of DVWA
- Introduction to WebGoat
- Configuring WebGoat
- Installation of Wamp Or Xampp
- Demonstration Of OWASP Top 10 On DVWA & WebGoat

PHP & JAVA Injection
- Introduction to PHP Injection
- Introduction to JAVA Injection
- Bypass Authentication using PHP & JAVA Injection
- Injection of Malicious Script Using PHP & Java Injection

CMS Hacking(Joomla, Wordpress)

- CMS Overview
- Introduction to Joomla & Wordpress
- Installation and Configuration of Joomla & Wordpress
- Control Panel Handling Of Joomla & Wordpress
- Your First Site In Joomla & Wordpress
- Hack CMS Using Vulnerable Plugings
- Countermeasures

Automatic & Maunal Vulnerability Finding
- Find Vulnerabilities Using Search Engines
- Vulnerabilities Findings Using Browser Addons & Plugings
- Tools For Finding Vulnerabilities
- Countermeasures

Web Scanners & Proxy (Hands on Practice)

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Accunetix
- Appscan
- Netsparker
- Havij
- Webscarab
- Burpsuite
- Zap Proxy

Sniffing & DNS-ARP Poisioning

- WireShark
- Cain & Abel
- Xplico
- Ettercap
- Network Miner

Session Hijacking

- HTTP Session Hijacking
- HTTPS Session Hijacking
- Cookie Stealing

URL & Website Virus Scanning

- URL Filtering & Scanning
- Web Site Scanning For Malicious Scripts
- Safe Surfing & Downloading Tips
- Browser Security

Designing Website Trackers

- What are Web Site Trackers?
- Custom Trackers
- Web Sites for Online Tracking
- Implementation of Tracker in Web Pages

Web Server(Apache, IIS) Vulnerability Testing

- Common Vulnerabilities in Web Servers
- Tool Based Testing
- Manual Testing
- Countermeasures

Ethical Hacking

Introduction To Ethical Hacking
- Overview Of Ethical Hacking
- Hackers Vs Ethical Hackers
- Different Types Of Hackers
- World Top Hacker's History
- Terminologies used in Hacking
- Malicious hacker phases
- Skills Required To Become a Hacker

Careers In Cyber Security
- Why Cyber Security is essential?
- Different Fields in Cyber Security
- Certifications and Importance
- Short & Long Term courses Available
- Need of Cyber Security Experts

Standard Pentesting Methodologies
- Description of different pen Testing Methodologies
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Open Web Application Security Project (OWASP) Top Ten
- Web Application Security Consortium Threat Classification (WASC-TC)

Understanding Cyber Law
- Overview Of Cyber Law
- Cyber Law India
- Need Of Cyber Law
- Cyber Crimes & Frauds
- Offences & Penalites
- Pros & cons Of Cyber Law

Footprinting, Information Gathering, Reconnaissance

- What is Information Gathering
- Active & Passive Information Gathering
- Google as a Information Gathering Agent
- Web based Footprinting
- Addons and Tool Based Footprinting

- Site For Footprinting

Hiding Identity(Proxy & vpn)

- Online Proxy
- Proxy Tools
- CGI Proxy
- Tab, Browser, System, Network Based Proxy
- VPNs
- Bypass Restrictions Using Proxy and VPNs

Scanning & Enumeration
- Overview of TCP/IP 3 way Handshake
- Stealth scans
- Nmap scanning methods
- Nmap Realworld scans
- Nmap Script Engine
- Evading firewall/ IDS
- Firewall scanning using HPING3
- Online Scanning
- Some useful scanners
- Autoscan, Superscan, Unicornscan
- Introduction to Enumeration
- SNMP Enumeration
- Banner grabbing

Advance Google Hacking
- Google and Its Working
- Dork For Google Hacking
- Tools For Google Hacking
- Web Crawling Tools
- Google as Vulnerability Scanner

System Virtualization & Cloning
- Virtualization
- Types Of Virtualization
- Vmware
- VirtualBox
- Backup & Restore
- Cloning

System Hacking(Windows XP, Windows 7 & 8)
- Password Cracking
- Password Resetting
- Login Without Entering Password
- Password In Plain Text
- Backdoor Installation
- Guest to Admin Login
- Securing System

Linux Hacking & Security
- Password Cracking
- Password Resetting
- Grub Password Hacking
- Linux Os Hardening
- Troubleshooting

Application Password Cracking
- Rar password cracking
- Ms Office Document Password Cracking
- FTP Password Cracking
- SSH Password Cracking
- Router & Switch Password Cracking

Steganography & Cryptography
- Introduction to Stenography
- Introduction to Cryptography
- Data Hiding Behind Images, Videos Files Etc
- Data Hiding Tools
- Cryptography
- Use of cryptography in Data Hiding

Exploitation By Malwares
- Introduction to viruses, Spywares, Trojans and Viruses
- Hacking Using Trojans and Others Malwares
- Binding Trojans
- Making Fully Undetectable Malwares and Others Viruses
- Bypassing Anti viruses
- Rootkits
- Botnets

Malware Analysis

- Overview Of Malware Analysis
- Manual Malware Analysis
- Tool Based Analysis
- Protection Against Malwares

Batch & Bash Programming
- Introduction to Batch & Bash Programing
- Designing Viruses in Batch
- Cookie and Information Grabber
- Automation Task
- Process Killer and Backdoor Designing

Email Hacking & Tracing Victim
- Session Hijacking
- Phishing
- Tabnabbing
- Clickjacking
- Fake Emailing
- Tracing Email
- Securing Accounts

Facebook, Yahoo & Gmail Hacking & Tracing Victim
- Profile Scanning
- Mobile Tracing by Facebook
- Fake profile Investigation
- Session Hijacking
- Phishing attack
- Social Engineering attack
- Tracing Victim
- Enhance Profile Security

Social Engineering Attacks
- What is Social Engineering
- Types of Social Engineering
- How to Perform Social Engineering Attack
- Prevention Against Social Engineering

Network Attacks & Security
- DOS & DDOS Attack
- DNS & ARP Poisoning
- Sniffing

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- SSL Striping
- Malwares
- Countermeasures

IDS, IPS & Honeypots
- IDS & IPS
- Installation, Configuration & Maintenance
- Honeypots
- Types Of Honeypots
- Implementation of Honeypots

Website Hacking & Countermeasures
- Bypass Authentication
- Manual & Automatic SQL Injection
- Cross Site Scripting
- Remote Code Execution
- Dumping Passwords
- Countermeasures

Database Hacking & Patching
- Introduction to Database
- Database Attacks & Countermeasures
- Cracking Of Phpmyadmin Panel
- Advance SQL Injection

Mobile Hacking & Tracing Location
- Call Spoofing
- Fake SMS
- Setting Local VOIP Server
- Mobile Location Tracing

Wireless Password Cracking
- WEP Cracking
- WPA/WPA2 Password Cracking
- WI-FI Router Password Cracking
- Wireless Security Measures

Vulnerability Assessment & Penetration Testing
- Introduction to VA-PT
- Key Benefits & Difference
- Closed Source VA-PT

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Opensource VA-PT
- Tool Based VA-PT
- Manual VA-PT

BackTrack & Bugtraq Based Exploitation & Testing
- Introduction to Back Track & Backtrack
- Installation, Configuration and Maintenance
- Exploitation by Backtrack & Bugtraq
- VA-PT By Backtrack & Bugtraq
- Troubleshooting

Miscellaneous
- Nexpose
- Core Impact
- Evilgrade
- Syringe Attack
- kautilya : Teensy Beyond Shells
- Cisco Global Exploiter

Digital & Cyber Forensic
- Chain of Custody reporting
- Acquisition
- Cloning
- Analysis
- Evidence Recovery
- Logs Analysis
- USB Forensics
- Wiping

Browser & Network Forensic
- Browser Password Cracking
- Browser History Recovery
- Browser Files Analysis For Evidence
- Network Forensic
- Network Traffic Analysis And Monitoring

Cyber Crime & Fraud Investigation
- Credit/Debit Card Frauds
- ATM Frauds
- Data & Domain Theft
- Fake Profiling & Emailing

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Miscellaneous Frauds & Investigation

Digital Forensics

Introduction to Computer Forensics
- Forensic Examination Procedures
- Introduction to Chain of Custody
- Preparing ur own Forensics tool kit
- Difference between IR & Forensics

Incidence Response
- IRM & forensics Life Cycle
- Windows Incidence Response
- Do's & Dont's in incidence response
- Different Methods of Live Acquisition
- Understanding Order of Volatality
- Memory Acquisition
- Analyzing Volatile Data
- Dynamic Disk Imaging
- Command based Acquisition
- Analyzing Windows Registry
- Analyzing Event viewer logs
- Imaging Volitaile data using netcat
- Verifying Memory dumps
- Analyzing Security policies

Linux Incidence response
- Understanding Linux Ext3/Ext4 file systems
- Understanding Boot process
- Boot problem cheat sheets
- Key differences between Windows & Linux
- Creating Response Toolkit
- Running Bash scripts to acquire live image
- Hash verification of output files

Forensics
- Types of Forensics
- Physical imaging Vs Logical imaging
- Understanding different methods of forensics duplication
- Traditional approach to forensics

Acquisition
- Methods of acquisition
- Imaging using encase
- Imaging using DEFT Linux
- Imaging using Helix
- Imaging using SIFT workstation
- Imaging using FTK

Analysis
- Understanding Metadata
- Analyzing swap & pagefiles
- Physical Analysis Vs Logical Analysis
- Mounting images to analysis tools
- Deleted file recovery
- Timestamp Analysis
- Analyzing Raw partitions
- Analyzing Stenographic data
- Understanding slacks
- String based searching
- Keyword based searching

Articulation
- Evidence collection
- Documenting Investigation process
- Timestamps Recording
- Hash calculations recording
- Do's and Don'ts

Browser Forensics
- Introduction to browser Forensics
- IE forensics
- IE log analysis
- Rebuilding IE cache & History
- Understanding Firefox logging & cache architecture
- Analyzing Firefox sqlite database
- Firefox Log Analysis
- Reconstructing Firefox cache & History
- Chrome Forensics
- Opera Forensics
- Tool based browser Forensics
- Using NetAnalysis, Blade, History Extractor

- Webhistorian
- Skype log Analysis
- Rebuilding skype chat

Network Forensics
Introduction to Network Foresnics
- Understanding network Architecture
- Understanding network Logging
- Investigating Wireless logs
- Investigating Network logs

Webserver log Analaysis
- IIS server Logs Architecture
- IIS log analysis using IE log Analyzer
- Apache Web server logging architecture
- Apache log analysis using apache log viewer

SIEM
- Introduction to SIEM
- Installing Splunk
- Configuring Splunk for weblogs
- Configuring Splunk for Network log analysis

Log Analaysis
- Understanding Firewall logs
- Configuring Syslog server
- Syslog log reading
- Cisco firewalls logging Methodology
- Cisco firewalls log analysis
- Understanding IDS Mechanism
- Overview of IDS Alerts & Sensors
- IDS log Analysis
- Router Forensics
- Router log analysis

Fraud & Forensics Analysis
- Cyber Laws
- Offences & Penalites
- Investigating Sexually Harassment cases
- Investigating Threat Mails
- E-Mail Tracking

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com

- Cyber Pornography

Case study
- Packet Analysis using wireshark
- Packet Analysis using Xplico
- Packet Analysis using NetworkMiner
- Test disk image analysis
- Participating Forensic challenges

Intrusion Detection System

Introduction to Snort

- Network Traffic Analysis using tcpdump and Wireshark
- TCP/IP Fundamentals
- Know your Enemy: How the bad guys attempt to penetrate your network
- Difference between HIDS & NIDS

Installing, configuring SNORT

- Configuration file
- Upgrading
- Sensor placement
- Logging
- Packet capture and analysis
- Preprocessors

Rule writing
- Dynamic rules
- Testing rules
- Optimizing rules
- Statistical analysis

Management tools
- Barnyard
- Snort console
- ACID
- Performance Tuning and thresholding
- Turning snort into an IPS

Logging and Analysis
- Log and Alert analysis
- Data Analysis Tools

- Installing and Using Barnyard

Security Onion
- Introduction to security onion
- Configuring Security onion
- Sensor Setup
- Configuring SGUIL server
- Configuring Snorby

Case Study
- Implementing NIDS to protect a network
- Implementing NIDS to secure Web application

ISO 27001

Introduction to ISO 27001
Differences between bs 7799 & ISO 27001
ISO 27001 domains
- Security Policy
- Security Organization
- Asset Management
- Human Resource Security
- Physical & Environmental security
- Communication & Operations management
- Access Controls
- System acquisition, Development & Maintenance
- Security incident Management
- Business Continuity Management
- Compliance
- PDCA cycle
- Implementation of ISO 27001

Hyderabad:
#201,202, Nagasuri Plaza, Above Bank of India, Mythrivanam, Ameerpet, Hyderabad, AP, INDIA.
Ph: 8686348800, 8686498081 | hyd@firewallearning.com, hr@firewallearning.com
Vishakapatnam:
3rd floor,G.K.towers, Opp: kalanikethan,R.T.C complex, Dwaraka nagar,Vishakapatnam, AP, INDIA.
Ph: 8686348811 / 33 | vzg@firewallearning.com