National Institute of Electronics and Information Technology Gorakhpur

Name of Group: IT Division

Name of Course: Enterprise Network Administration & System Security (A Practical Approach)

Objective:
This training facilitates classroom and laboratory learning, letting candidates to develop competence and confidence in administrating, customizing and securing Windows & Linux based Systems as well as routing and switching in an enterprise network.
The technical content of the course gives a broad overview of essential concepts and methods for providing and evaluating security in Windows/Linux based system and Routing, Switching. This training also provides an environment to learn anatomy of ethical hacking and designing of countermeasures against various types of attacks.

Duration: 6 Weeks

Eligibility: B.TECH. (CS/IT/EC/EE) or MCA/M.Sc. (IT/CS/Electronics), BCA /PGDCA, Diploma in Computer /Electronics Stream, B.Sc. or B.A, A/B/C Level, Working Professional. Basic knowledge of computing is desirable

Course Fees (Proposed): Rs. 1000/- per week (+ GST)

Registration Process: Candidates have to apply in prescribed application form. The forms can be collected from NIELIT Gorakhpur centre or can be downloaded from the NIELIT Gorakhpur website. The duly filled form along with the course fees has to be submitted at NIELIT Gorakhpur centre. The Fees deposited is Non-Refundable.

Course Content:

Modules:	Duration	Contents
Module 1	6 Week	• System Administration & Security using Windows Server 2012 • Linux System Security & Administration • Data Communication (Routing & Switching) • Information Security

* There will be 3 Hours Session per day.
* These sessions will include Theory Classes, Demo and Practical.

Mode of Payment: Fees can be paid either by swiping debit/credit card or by challan.

For any queries and more details please contact
Sh. Abhinav Mishra**(8317093868)**
Md. Yousuf **(8317093886)**

6 Weeks Summer Training Program in Enterprise Network Administration & System Security

(A Practical Approach)

राष्ट्रीय इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी संस्थान, गोरखपुर
National Institute of Electronics and Information Technology (NIELIT) Gorakhpur
An Autonomous Scientific Institution of
Ministry of Electronics & Information Technology (MeitY), Govt. of India
Deoria Road, M. M. M. University of Technology Campus,
Gorakhpur, U.P.– 273010
Web: http://nielit.gov.in/gorakhpur/

Approach)			
1	**Course Descriptions**	This course will provide an overview on Windows 2012 Server, Linux Security and Administration. In this course, the candidate will learn how to implement and manage Windows 2012 R2 system in their IT infrastructure and securing the services in Windows/Linux based operating system. The candidate would also go through Routing and Switching implementation. The technical content of the course gives a broad overview of essential concepts and methods for providing and evaluating security in Windows & Linux based system. This course also provides an overview on Routing, Switching and Security Technology. This course will learn how to secure WAN implementation. This is an intensive, practical "hands-on" training where participants would gain the skills in various area of information security such as Information gathering, ARP cache poisoning and MITM attack, Brute force attack, Denial of Service (DoS) attack, IP Spoofing, root kits, SQL Injection, Code Injection, E-mail spoofing & Phishing, E-mail security using PGP, configuring snort IDS, IPSec, IP tables, Hardening windows & Linux and finally evaluating Security.	
2	**Objective**	This training facilitates classroom and laboratory learning, letting candidates to develop competence and confidence in administrating, customizing and securing Windows& Linux based Systems as well as routing and switching in an enterprise network. This training also tests a candidate's knowledge and skills required installing, operating, and troubleshooting a small to medium size enterprise branch network. This training also provides an environment to learn anatomy of ethical hacking and designing of countermeasures against various type of attacks.	
3	**Target Users/ Sections**	▪ Government officers	▪ Govt Department
		▪ Technical Officer	▪ Diploma Scholars
		▪ Programmer	▪ UG/PG Scholars
		▪ Network Administrator	▪ Police Department
		▪ System Administrator	▪ Legal Department
4	**Intake**	Twenty Five (25)	
5	**Duration**	6 Weeks/ 3 Hrs daily	
6	**Topic that would be Covered**	• Windows 2012 Server Administration • Securing Services in Windows 2012 Server • Linux System Administration • Securing Services in Linux	• Routing • Switching • Information Security • Network Security
7	**Training Fee**	Rs 6,000.00 (Excluding applicable GST) The course fee may be submitted in online mode through NEFTY/RTGS/BANK TRANSFER in following account of NIELIT GORAKHPUR. Account Holder :NIELIT Gorakhpur Branch: Kunraghat ,Gorakhpur -273009 A/C Type: CURRENT A/c No: 1914002100094252 Bank : Punjab National Bank IFSC Code:PUNBB0191400	
8	**Eligibility**	Basic working knowledge of Operating System. ,UG/PG Engineering(CS/IT/EC/EI/EE), Diploma (CS/IT/EC)Scholars	
9	**Training**	By the end of this course the candidates should have developed an understanding of:	

	Outcomes	• Networking and its components • TCP/IP troubleshooting utilities. • Deployment of Windows Server 2012 • NTFS Security • Deployment of DNS ,DNSSEC and DHCP • Deployment and Securing of IIS web server • Implementation of IPSec, NAP • Using VPN,NAT through RRAS • Securing Active Directory. • Static and Dynamic Routing Protocol • Switching and VLAN • ACL • Linux System Administration • Deployment of Telnet, SSH, FTP, SAMBA Implementation of DNS,DHCP • Securing Services in Linux • Setting up Apache and Squid Proxy Server • Firewall using iptables	• Implementing Static Routing and Dynamic Routing • Configuring Access Control List to control the traffic • Securing Wireless Network • Information Gathering & Countermeasures • Sniffing & Countermeasures • Brute Force Attack & Countermeasures • IP Spoofing with DoS & Countermeasures • Trojan, Backdoor & Virus& Countermeasures. • Bypassing Proxy& Countermeasures • SQL Injection Attack & Countermeasures • E-mail Spoofing, Phishing & Countermeasures • E-mail Security • Network Traffic Encryption • IDS • Syslog • Network Security

For More Information

Mohd Yousuf Senior Technical Officer Mobile: 8317093886 e-mail: yousuf@nielit.gov.in	Abhinav Mishra Scientist C Mobile: 8317093868 e-mail: abhinav@nielit.gov.in

Course Contents

MODULE A: SYSTEM SADMINISTRATION & SECURITY USING WINDOWS SERVER 2012

Unit 1	**Basic Networking**
	Introduction to Computer Networks: Element of Networks, Types of Networks, Network operating system Vs Client operating System,
	Transmission Media: Guided Media Vs Unguided Media, Common LAN Media (STP, UTP, Coaxial cable, and Optical fiber) TIA/EIA standards, Making & testing Cable, Straight thru Cable, Crossover Cable, and Connectors.
	Networking Devices: NIC, Repeaters, Hub, Switches, Routers, and Converter etc. Internetworking Vs Internetworking Devices, Collision Domain Vs Broadcast Domains, Security in Hub, Switch.
	Internet Protocols: OSI Model, TCP/IP Model
	TCP/IP Troubleshooting utilities Uses of ping, arp, traces route, tracert, nslookup, netstat etc. Troubleshooting IP Addressing. Subnetting ICMP. TCP/IP troubleshooting command line utilities, Introduction to Transport layer, TCP and UDP Protocols, Port No. Socket Address, TCP & UDP Port No, Port types.
	IP Addressing: IP Addressing, IP Terminology, IP address Classes, IP Addressing Scheme, Public & private IP address, Basics of Subnetting, and Subnet Masking. IPv4 vs IPv6 comparison
	Internet Internet, connection types, ISP, ISP study, Web hosting, Top Web Hosting Companies in India performing whois to get IP by name, Name by IP & IP address owner information , IANA, IANA Root Zone Database, IANA Number Resources, local Internet registry (LIR),National Internet Registry (NIR), AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC, Regional Internet Registry (RIR),Registration of a domain, Top Domain Registrars, Registrar for .EDU.IN, .RES.IN, .AC.IN, .GOV.IN in INDIA
Unit 2	**Introduction to Windows Server 2012** Windows 2012 server family, Windows Server 2012 Standard Edition, Windows Server 2012 Enterprise Edition ,Windows Server 2012 Datacenter Edition, Windows Web Server 2012 Performing a Clean Installation, Performing an Upgrade Installation
	NTFS File System and Security Sharing file & folder, managing file and folder attributes. Managing shared folder permissions. Overview of NTFS permissions, implementing and configuring NTFS permissions, access control list (ACL), access control entry (ACE),Adding and Removing NTFS Permissions for users/Groups, Advanced Permissions, Cumulative Permissions, NTFS Permissions Inheritance, Files/Folders Ownership, Effective Access, Configuring NTFS Permissions, Overview Of Share Permissions, Combining NTFS And Share Permissions, Overview Of Encrypting File System (Efs) User and group and its Permissions, Managing NTFS file and folder security, NTFS permissions, EFS. How user and group NTFS permissions combine, Taking ownership of files and folders.
Unit 3	**DHCP Overview** DHCP Operation , APIPA, Adding Role of DHCP Server, Configuration, DHCP Scope, Super scope, Reservation, DHCP testing and troubleshooting, DHCP Server monitoring, Monitoring DHCP Pool utilization, finding unauthorized DHCP Servers

	Introduction to DNS The elements of a domain name, The DNS namespace, TLDs, gTLDs, registering domains, Name servers, how DNS works. DNS port numbers, DNS queries, Zone transfer (AXFR and IXFR),NOTIFY, Domains and Zones, Forward Mapping, Reverse Mapping, Zone File ,Resource Records (RRs),SOA RR,NS RR,MX RR,CNAME RR,A (IPv4) and AAAA (IPv6) RRs, PTR RR,TXT RR DNS Server configuration Primary & secondary DNS Server, Forward lookup zones and reverse lookup zone, Root Hints, Zone Transfer,
	DNS Security Basics DNS Protocol Vulnerabilities, DNS Spoofing, cache poisoning, Man in The Middle Attacks, Security threat analysis, DNS security scope (Zone transfer, DDNS, zone integrity),Stealth configuration, Restricting queries, DNS and firewalls, Split DNS, forwarders, internal root servers
Unit 4	**Introduction to IIS** Components of IIS, IIS Web server, Configuring a website ,Configuring multiple website using multiple IP address, Virtual directory and multiple ports, Configuring a FTP site, Configuring multiple ftp sites using multiple IP address, Virtual directory and multiple ports **Securing IIS** IP Address and Domain Restrictions, Server Certificates and SSL,Enabling SSL/TLS for secure data communications Securing Web Content, Enabling user authentication, Removing anonymous access, Selecting appropriate authentication modules, Restricting access to sensitive content Authorization, URL-Based Authorization
	Routing and Remote Access Configuring Network Access, Configuring VPN Access, Overview of Network Policies, Troubleshooting Routing and Remote Access, Configuring and Managing Network Access, Configuring Routing and Remote Access as a VPN Remote Access Solution, Configuring a Custom Network Policy, Configuring Logging, Configuring a Connection Profile
	Implementing IPSec Introduction to IPSec, benefits and uses of IPSec, IPSec Operation Modes ,Tunnel Mode ,Transport Mode , IPSec Encryption Methods ,Encapsulating Security Payload (ESP) ,Authentication Header (AH) Securing Network Traffic using IPSec in Windows 2012
Unit 5	**Active Directory** Understanding the Features of Active Directory. Naming conventions logical structure of Active Directory. Windows 2012 R2 domain organizational units (OUs), trees and forests. Objects and classes, schema, global catalog server. Installing Active Directory, Domain function levels. What does DNS have to do with Active Directory? Verifying and troubleshooting an Active Directory installation. Organizational Unit (OU), Creating OUs, configuring OU, properties. Managing Active Directory objects. Active Directory Certificate Services. **Group Policy** Introduction to Group Policy. How to configure Group Policy. Securing Windows Servers Using Group Policy Objects, Configuring Security Settings, Restricting Software. **Read-Only Domain Controllers** Read-Only Domain Controller Operation, Deploying an RODC,Administering an RODC
Module B: Linux System Security & Administration	
Unit 1	**LINUX INTRODUCTION AND FILE SYSTEM** The CentOS Linux File system, The CentOS Shell, The CentOS Linux Utilities **INSTALLING CENTOS 6** Server Preparing for the Installation, Configuring the Server's Hard Drive, Starting the CentOS Server Installation Process, Completing the Installation **COMMAND LINE UTILITIES** Working as root, working with the Shell, Using Bash to Best Effect, Managing Bash with Key Sequences, Performing Basic File System Management Tasks, Working with Directories, Working with Files, Viewing the Content of Text Files, Finding Files That Contain Specific Text , Creating Empty Files, Piping and Redirection, Piping, Redirection, Finding Files, Working with Vi Editor: Vi Modes, Saving and Quitting, Cut, Copy, and Paste, Deleting Text. Getting Help:Using man to Get Help, Getting Information on Installed Package
Unit 2	**MANAGING USERS AND GROUPS ACL** Setting Up User Accounts, Commands for User Management, Managing Passwords, Modifying and Deleting User Accounts, Configuration Files, Creating Groups, Commands for Group Management, /etc/group, Using Group Passwords, Managing the User's Shell Environment, Configuring Permissions, Read, Write, and Execute: The Three Basic Linux Permissions, Permissions and the Concept of Ownership, Working with Advanced Linux Permissions, Setting Permissions, Using unmask to Set Default Permissions for New Files, Working with Access Control Lists, Preparing the File System for ACLs, ACL Limitations, Applying File Attributes, Apply Quota to Allow a Maximum Amount of Files, Installing the Quota Software, Preparing the File System for Quota, Initializing Quota, Setting Quota for Users and Groups, Configuring Administrator Tasks with sudo **FILE SYSTEM MANAGEMENT BASIC** Mounting Disks, Using the mount Command, Unmounting Devices, Automating Mounts with /etc/fstab, Checking File System Integrity, Working with Links: Working with Symbolic Links, Working with Hard Links. Configuring Storage, Comparing File Systems, Creating File Systems, Working with Logical Volumes **PROCESS AND BOOT PROCESS** Process Monitoring and Management, Different Kinds of Processes, Foreground and Background, Managing Processes Other Tools to Monitor System Activity, Setting Process Priority, Executing Processes Automatically, Configuring cron,Executing Once with at, Tuning the Boot Procedure, Managing the GRUB Boot Loader, The GRUB Configuration File, Installing GRUB, Working with the GRUB Boot Menu, Runlevels, Hardware Management with udev
Unit 3	**CONFIGURING NETWORK INTERFACE** Configuring the Network Card, Using ifup, ifdown, and Related Tools, Using ifconfig, Using the ip Tool, Configuring the DNS Resolver, Configuring Network Card Properties with the ethtool Command, Troubleshooting Network Connections, Testing Connectivity, Testing Availability of Services, Monitoring the Network Interface.

	SOFTWARE PACKAGE MANAGEMENT Software Management, Software Repositories and Package Databases, Package Management Utilities, Using apt, Installing Software from Tarballs, Configuring a Graphical User Interface, Creating Backups, Making File Backups with tar, Making Device Backups Using dd, Configuring Logging, Configuring syslog **TELNET** **SSH**	
Unit 4	**FTP** **SAMBA** Sharing Files with Samba, Samba Server Possibilities and Impossibilities, Configuring the Samba Server, Client Access to the Samba Server **NFS** Sharing Files with NFS, Using the NFS Server, Understanding How the NFS Works, Configuring an NFS Server, Configuring an NFS Client, Monitoring the NFS Server **DHCP** Configuring DHCP, Understanding the DHCP Protocol, Creating the DHCP Server Configuration, The DHCP Process, The /etc/dhcp/dhcpd.conf Configuration File, Advanced DHCP Configuration Options **DNS** DNS Hierarchy, Introducing Forward and Reverse DNS, Configuring DNS, Configuring Reversed Lookup, Testing Your Name Server	
Unit 5	**APACHE** Setting up Apache, Apache Components, Starting, Stopping, and Testing the Apache Web Server, The Structure of the Apache Configuration Files, Checking the Configuration, Working with Virtual Hosts, Configuring Virtual Hosts, Managing Access to the Web Server, Configuring Host-Based Access Restrictions, Configuring User-Based Access Restrictions **SQUID PROXY** Configuring a Squid Proxy Server, Installing a Squid Proxy Cache, Configuring Squid Access Control Policies, Configuring User Authentication **FIREWALL USING IPTABLES** Using iptables to create a Firewall **SETTING UP MAIL SERVER** SMTP**,** POP3,IMAP, Postfix	
Module C:Data Communication (Routing & Switching		
Unit 1	Internetworking Basics, Broadcast domain, Collision Domain, Hub, Switch & Router ,Ethernet Cabling: - Straight-Through Cable, Crossover Cable, Rolled Cable Internet Protocols: - TCP/IP Model, IP Addressing, IP Terminology, IP Addressing Scheme, Private IP Addresses ,TCP/IP Troubleshooting utilities, Troubleshooting IP Addressing IP Sub netting and Variable Length Subnet Masks (VLSM) .Sub netting Basics, How to Create Subnets, Subnet Masks, Classless Inter-Domain Routing (CIDR), Sub netting Class C Addresses, Sub netting Class B Addresses, Sub netting(VLSMs), VLSM Design, Implementing VLSM Network	
Unit 2	Introduction to the Cisco IOS the Cisco Router User Interface, Cisco Router IOS, Connecting to a Cisco Router, Bringing up a Router, Setup Mode, Command-Line Interface, Logging into the Router, Overview of Router Modes, CLI Prompts, Basic commands IP Routing, Routing Basics, Static Routing, Default Routing, Dynamic Routing, Routing Protocol Basics, Administrative Distances, Routing Protocols, Distance-Vector Routing Protocols, Maximum Hop Count, Route Poisoning , Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP) Enhanced IGRP (EIGRP) and Open Shortest Path First (OSPF) EIGRP Features and Operation, Open Shortest Path First (OSPF) Basics	
Unit 3	Switch Configuration, Layer 2 Switching Switching basics, Configuring the Catalyst 1900 and 2950 Switches,1900 and 2950 Switch Startup, Setting the Passwords, Setting the Hostname, Setting IP Information, Configuring Interface Descriptions,Erasing the Switch Configuration Virtual LANs, VLAN Basics, Broadcast Control, Security ,Flexibility and Scalability ,VLAN Memberships, Static VLANs ,Dynamic VLANs, Identifying VLANs, Frame Tagging, LAN Identification Methods , Inter-Switch Link (ISL) Protocol ,VLAN Trunking Protocol (VTP),VTP Modes of Operation, VTP Pruning, Routing between VLANs ,Configuring VLANs, Assigning Switch Ports to VLANs ,Configuring Trunk Ports ,Configuring Inter- VLAN Routing, Configuring VTP.	
Unit 4	Cisco Router ,Managing a Cisco Internetwork The Internal Components of a Cisco Router, The Router Boot Sequence Understanding the Configuration Register Bits, Checking the Current Configuration Register Value, Changing the Configuration Register, Recovering Passwords, Backing Up and Restoring the Cisco IOS, Verifying Flash Memory, Backing Up the Cisco IOS, Restoring or Upgrading the Cisco Router IOS ,Backing Up and Restoring the Cisco Configuration, Erasing the Configuration ISM band, Managing Traffic with Access Lists Introduction to Access Lists, Standard Access Lists, Wildcard Masking, Standard Access List Example, Controlling VTY (Telnet) Access, Extended Access Lists, Extended Access List Example, Named Access Lists, Monitoring Access Lists	
Unit 5	NETWORK ADDRESS TRANSLATION (NAT), Network Address translation NAT, Introduction to Network addresses Translation (NAT), Port address translation (PAT), Static NAT, Dynamic NAT, NAT Overloading ISM band, ISM band, 802.11a/b/g wireless standards, Adhoc, infrastructure mode of WLAN, Access Point in Repeater Mode,Security in WLAN, MAC Filtering, WEP/WPA.	
Module D: Information Security		
Group A (Information Gathering & Countermeasures)		
M1	Information Gathering & Countermeasures	• To Understand Information Gathering, Network Discovery & Scanning Target Enumeration, Vulnerability Assessment • Hands-on lab

Group B (Anatomy of Hacking & Countermeasures)		
M2	Sniffing & Countermeasures	• To Understand Sniffing, Man in the Middle Attack (MITM) and ARP Cache Poisoning • Hands-on lab for ARP Cache Poisoning & Sniffing
M3	Brute Force Attack & Countermeasures	• To Understand Hash Function, Password Hashes, Brute Force Attack and Types of Password Attacks • Hands-on lab for Brute Force Attack
M4	IP Spoofing with DoS & Countermeasures	• To Understand Spoofing, IP Spoofing and Denial of Service (DoS) • Hands-on lab for IP Spoofing and DoS
M5	Trojan, Backdoor & Virus& Countermeasures.	• To Understand Trojan, Backdoor and Viruses • Hands-on lab of Trojan Attack for Windows Operating System
M6	Bypassing Proxy& Countermeasures	• To Understand Spoofing Proxy Servers, Types of Proxy Servers and Web/Content Filtering • Hands-on lab to Bypassing Proxy & Countermeasures
M7	SQL Injection Attack & Countermeasures	• To Understand SQL Injection, Plain SQL Injection, Blind SQL, Injection Preventive Measures and Data Validation • Hands-on lab for SQL Injection Attacks & Countermeasures
M8	Code Injection & Countermeasures	• To Understand Code Injection, Types of Code Injection and DLL • Hands-on lab for Code Injection: Static Code Injection
M9	E-mail Spoofing, Phishing & Countermeasures	• To Understand E-mail Spoofing, Phishing and Phishing Techniques • Hands-on lab for E-mail Spoofing, Phishing & Countermeasures
M10	Hacking Wireless Network &Countermeasure	• To Understand Wireless Network Attacks, Scanning Wireless Network and Cracking WEP/WPA Key of Wireless Network • Hands-on lab for Hacking Wireless Network & Countermeasures
Group C (Hardening, Perimeter Security & Evaluating Security)		
M11	E-mail Security	• To Understand Common E-mail Protocols, E-mail Encryption and Digital Signature • Hands-on lab for E-mail Security
M12	Network Traffic Analysis	• To Understand Network Traffic Analysis • Hands-on lab for Network Traffic Analysis
M13	Network Traffic Encryption	• To Understand IP Security, Protocols used in IPSec, Security Architecture of IPSec and Modes of IPSec • Hands-on lab for IP Security
M14	Installing & Configuring Intrusion Detection System	• To Understand Intrusion Detection System, Various Types of IDS and Components used in Snort Implementation • Hands-on lab for Installing & Configuring IDS using snort and OSSEC
M15	Configuring Host Based Firewall	• To Understand Basic concepts of Firewall, Basic techniques for Configuring Firewall • Hands-on lab to Configuring Host Based Firewall (Windows) and Firewall (Linux)
M16	Host System Hardening (Windows)	• To Understand Vulnerability Assessment and OS Hardening • Hands-on lab for Windows Server Hardening
M17	Host System Hardening (Linux)	• To Understand OS Hardening • Hands-on lab for Linux Hardening
M18	Evaluating Security	• To Understand Security Evaluation, Penetration Testing and Benefits of Penetration Testing. • Hands-on lab for Windows Server Penetration Testing
M19	Log Analysis using Syslog	• To Understand Log Analysis using Syslog • Hands-on lab on Syslog.
MODULE E:Miscellaneous Hands on Network Security (A/N Session)		
Network Security		• Preventing CAM Flooding Attacks by using Switch Port Security • Preventing unauthorized access to DHCP Server by using DHCP Snooping • Preventing MAC Spoofing by using IP Source Binding. • Configuring traffic Access Control using Standard ACL • Controlling Access to Remote Administration Services using (ACLs) • Configuring Traffic Access Control using Extended ACL • Configuring Site to site VPN configuration using IPSec • Configuring Lock down of LAN, WAN and DMZ Zone using pfSense