National Institute of Electronics & Information Technology
Gorakhpur – Extension Centre Lucknow
(Under Ministry of Electronics and Information Technology, Govt. of India)
MMMUT Campus, Deoria Road, Gorakhpur-273010
https://www.nielit.gov.in/gorakhpur/

Ethical Hacking & Information Security

Ethical Hacking and Information Security

4 Weeks Online Course

4 Weeks. (3 Hrs. per day)

Medium of Instruction: Bilingual (English& Hindi)

Objective

This course introduces the concepts of Ethical Hacking and gives the learner the opportunity to learn about different tools and techniques in Ethical hacking and security and to identify and analyze the stages an ethical hacker requires to take in order to compromise a target system as well as will apply preventive, corrective and protective measures to safeguard the system. After the completion of this course, candidate would be able to identify tools and techniques to carry out a penetration testing and critically evaluate security techniques used to protect system and user data and it will also help to demonstrate systematic understanding of the concepts of security at the level of policy and strategy in a computer system.

Eligibility

B.E*/B.Tech.* / B.Sc. - M.Sc. / Graduate / Diploma in any stream with Basic Knowledge of Programming or B.C.A*. / M.C.A. pursuing or qualified or NIELIT O-Level / NIELIT A-Level Qualified or 10+2 qualified with knowledge of programming. **(Note: *pursuing candidate can also apply)**

Prerequisites

- ✓ Candidate must have latest computer/laptop with preferably 4 GB RAM or higher
- ✓ Internet connection with good speed *(preferably 2 Mbps or higher).*

Course Fees

Rs. 3700/- incl. GST & all other charges.

Certificate

Hard Copy of Certificate will be provided to the participants, based on minimum 75% attendance and on performance (minimum 50% marks) in the online test, conducted at the end of the course.

Methodology

- ✓ Instructor-led live classes.
- ✓ Instructor-led hands-on lab sessions using **Virtual Lab**.
- ✓ Content Access through e-Learning portal.
- ✓ Assessment and Certification

How to Apply

Step-1: Read the course structure & course requirements carefully.

Step-2: Visit the Registration portal and click on apply button.

Step-3: Create your login credentials and fill up all the details, see the preview and submit the form.

Step-4: Login with your credentials to verify the mobile number, email ID and then upload the documents, Lock the profile and Pay the Fees online, using ATM-Debit Card / Credit Card / Internet Banking / UPI etc.

Course Content

Day	Topic	Day	Topic	Day	Topic
Day #01	NETWORK PRIMER -I	Day #02	NETWORK PRIMER –II	Day #03	NETWORK PRIMER –III
Day #04	EXPLORING NMAP AND WIRESHARK	Day #05	INFORMATION GATHERING AND COUNTERMEASURES	Day #06	SNIFFING, ARP CACHE POISONING , MITM ATTACKS AND COUNTERMEASURES
Day #07	PASSWORD CRACKING AND COUNTERMEASURES	Day #08	IP SPOOFING, DENIAL OF SERVICE AND COUNTERMEASURES	Day #09	TROJAN, BACKDOOR, VIRUS AND COUNTERMEASURES
Day #10	STEGANOGRAPHY	Day #11	E-MAIL SPOOFING, PHISHING AND COUNTERMEASURES	Day #12	SECURING E-MAIL COMMUNICATION USING PGP
Day #13a	WEB APPLICATION PRIMER	Day #13b	WEB APPLICATION SECURITY –I	Day #14	WEB APPLICATION SECURITY –II
Day #15	WEB APPLICATION SECURITY -III	Day #16	NETWORK TRAFFIC ENCRYPTION USING IPSec	Day #17	INTRUSION DETECTION SYSTEM USING SNORT
Day #18	NETWORK SECURITY-I	Day #19	NETWORK SECURITY-II	Day #20	PENETRATION TESTING USING METASPLOIT

Course Coordinator

Sh. Abhinav Mishra (Scientist D),
NIELIT Gorakhpur,
Email: abhinav@nielit.gov.in
Mobile Number: 8317093868

Sh. Pawan Verma,STO
NIELIT Lucknow,
Email: pawanverma@nielit.gov.in
Mobile Number: 7706009310

Course Contents

Day	Detailed Conceptual Topic	Hands On lab
Day1	**NETWORK PRIMER -I** What is Networking, Benefits of Network, Components Of Computer Network, Client/Server Model, Types of Servers, Role of A Network Administrator, Internetwork, Network Segmentation, LAN traffic congestion, Collision Domains, Broadcast Domain, Transmission modes, Ethernet, CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Classification Of Transmission Media, Coaxial Cable, Twisted-pair cables, STP and UTP cables, Categories of Twisted cable, Cabling types, UTP Categories, Exploring UTP, Categories of Ethernet Cable, Fiber Optics Cable, OFC Connectors, Types of Fiber Optics Cable, Single vs Multi-Mode Fiber, Ethernet Cabling, Straight-Through Cable, Crossover Cable, Rolled over Cable, Causes of Transmission Impairment. Repeaters, Switch, MAC-Port Binding, Repeater, Hub,Bridge, Switch, Router, L3 Switch OSI Reference Model, Layers of the OSI Reference Model, Application Layer (Layer 7), Presentation Layer (Layer 6), Session Layer (Layer 5), Transport Layer (Layer 4), TCP, UDP, Reliable Communication with TCP, 3-Way Handshake, The TCP Sliding Window, Port Numbers, Common TCP& UDP Ports, Network Layer (Layer 3), Data Link Layer (Layer 2), Physical Layer(Layer 1), OSI Upper Layer & Bottom Layer, OSI Layer Functions OSI PDU Term, Maximum transmission unit Checking with MTU, Changing the MTU size in Windows, Path MTU Discovery (PMTUD),Maximum Segment Size (MSS), Devices at OSI layer TCP/IP, The roots of the internet, Some important TCP/IP milestones, MAC Address, Vendor / Ethernet/ Bluetooth MAC Address Lookup, MAC Address Format, IP Address, Physical Vs Logical Address, ARP Protocol TCP Header format, TCP Flags, UDP Header Format, IPv4 Header, Common Protocol Number, ICMP Protocol, Ethernet Frame Format, IP Address, Classes, IP Addressing Scheme	• Study of Ethernet Cabling: - Straight-Through Cable, Crossover Cable, Rolled Cable. • Verifying MTU of Network • Changing the MTU size in OS.
Day2	**NETWORK PRIMER -II** Subnetting Basics, How to Create Subnets, Subnet Masks, Classless Inter-Domain Routing (CIDR), Subnetting Class C Addresses, Subnetting Class B Addresses, Physical Vs Logical Address, Public & Private IP Addresses	• Practice on IP Subnetting on CLASS A,B & C networks.
Day3	**NETWORK PRIMER –III** IANA, Regional Internet Registry (RIR), local Internet registry (LIR), National Internet Registry (NIR), AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC, Indian Registry for Internet Names and Numbers (IRINN), Internet Exchange Point, IANA Root Zone Database, IANA Number Resources, Regional Internet Registry (RIR),Internet, Network Registrar for .EDU.IN, .RES.IN, .AC.IN, .GOV.IN, List of Root Servers, Internet in India , SEA-ME-WE3,TCP/IP Troubleshooting utilities, Troubleshooting IP Addressing, hostname, ipconfig/ ifconfig / winipcfg, arp, ICMP Protocol, ICMP Protocol -Type, Ping, TTL, Default TTL Values, Changing the TTL On Popular Operating Systems, Ping Command Error Messages ,tracert/traceroute, Pathping, route, netstat, Possible Session States in netstat output,getmac,nslookup, DNS Resource Records, Troubleshooting IP Addressing	• Hands-on lab on Whois Domain Lookup, Whois IP lookup. • Hands-on lab on Nslookup ,TCP/IP Utilities, hostname, Arp, Ping, tracert / traceroute, Netstat, Getmac, Nslookup
Day4	**EXPLORING NMAP AND WIRESHARK** Introduction to NMAP, Exploring Scanning using NMAP, NMAP Advanced Scanning Techniques, Introduction to Wireshark, Functionality of Wireshark, UI of Wireshark, Wireshark Capture Mode, Capturing Packets, Wireshark Filters, Detecting Network Attacks with Wireshark, Detection of host discovery (recon), Detection of network port scanning, Detection of wireless network attacks	• Hands-on lab on NMAP and Wireshark
Day5	**INFORMATION GATHERING AND COUNTERMEASURES** Introduction to Ethical Hacking, What is hacking?, Definition of Hacking, Types of Hackers Introduction to Information Security, CIA Triad, Services & Techniques, Actives, Passive Threats and Exploit, etc. Introduction to Information Gathering, Phases of Information Gathering, Reconnaissance, Banner Grabbing, Web Ripping, Website at Offline Mode, Downloading Server Side Code, Foot Printing, Name Space Lookup,Trace Routing Techniques, Whois Lookup Query, Fingerprinting Registration details of the website, contact details. Finding out the target IP address, Finding out DNS record, sub-domains, Operating system, Finding login pages, Finding out sensitive, directory, Find out any known vulnerability Network Scanning, Network Scanning Techniques and Scanning countermeasures.	• Hands-on lab on Information Gathering , NMAP Scanning, Whois, nslookup and its countermeasures
Day6	**SNIFFING, ARP CACHE POISONING, MITM ATTACKS. AND COUNTERMEASURES** ARP Protocol, Sniffing ARP Cache Poisoning, Man in the Middle (MITM) Attacks, Type of MITM Attacks, Scenario for Sniffing & ARP Cache Poisoning, Countermeasures for Sniffing & ARP Cache Poisoning	Hands-on Lab on Sniffing, ARP Cache Poisoning, Man in the Middle (MITM) Attacks using ettercap & its Countermeasures

Day7	**PASSWORD CRACKING AND COUNTERMEASURES** Hash function, Hash algorithm, Password Hashes, Types of password attacks, Password Cracking types, Dictionary Attack, Brute Force Attack, Hybrid Attack, Rainbow Table Attacks, Cracking Passwords using John the Ripper, Other password Cracking tools, How passwords are stored in Linux,/etc/passwd and /etc/shadow, Permissions of /etc/passwd and /etc/shadow, Salt, Displaying hashing Algorithm used in Linux, pwconv, and pwunconv, How passwords are stored in Windows, SSH Password Testing With Hydra, THC Hydra Commands, Hardening of SSH, Password Cracking Countermeasures.	Hands-on lab on Password cracking techniques, Password Testing With Hydra,exploring,/etc/passwd and /etc/shadow and its countermeasures
Day8	**IP SPOOFING, DENIAL OF SERVICE, AND COUNTERMEASURES** IP Spoofing, Denial of Service (DoS), TCP SYN Flood Attack using hping3,Detecting TCP Syn Flood attacks using Wireshark, Detecting TCP Syn Flood attacks using netstat, Suggesting & Implementing Countermeasures	Hands-on lab on IP Spoofing, Denial of Service (DoS) ,hping, netstat, and its countermeasures
Day9	**TROJAN, BACKDOOR, VIRUS, AND COUNTERMEASURES** Introduction to Virus, What is Trojan?, Types Of Trojans, Different way a Trojan Can Get Into A System, Trojan, Backdoor, What is Keylogger, Categorization of Keystroke Loggers& Virus & Countermeasures,	Hands-on lab on Trojan, Backdoor and its countermeasures
Day10	**STEGANOGRAPHY** Information Hiding, Techniques Steganography, Information Hiding Techniques, Steganography, Types of Steganography, Difference Between Steganography and Cryptography, Steganography with CMD.Best Tools to Perform Steganography, Steganography using image file Steghide tool, Steganography with CMD, Steganography using image file Steghide tool, Scapy tool used for Steganography, ICMP, Steganography using ICMP Payload Scapy tool used for Steganography	Hands-on lab on Steganography CMD and using an image file Steganography using ICMP Payload
Day11	**E-MAIL SPOOFING, PHISHING, AND COUNTERMEASURES** Concept of Email, SMTP, POP3 and IMAP, Email Spoofing, Types of Phishing, E-mail Phishing, E-Mail Tracking by Header, Concept of Fake E-mails, Protections, SPF,DKIM and DMARC records, Using nslookup to check SPF/DKIM/DMARC records Concept of Fake E-mails	Hands-on lab on demonstration on phishing mail and its countermeasures.
Day12	**SECURING E-MAIL COMMUNICATION USING PGP** PGP, E-mail Security, Securing E-Mail Communication, PGP,MIME,S/MIME, Difference between PGP and S/MIME, Scenario For E-mail Security	Hands on lab on Securing E-Mail communications using PGP
Day13a	**WEB APPLICATION PRIMER** Web Application Primer, Working of website, Application ,WWW (World Wide Web), ,Types of website - Static Website, Dynamic Website, Front End, Back End, Scripting Language, Responsive Web Design (RWD),HTTP Protocol, Basic Features of HTTP, HTTP Version, HTTP Request / Response , URI , URL , URN, Cookies, Session, HTTP Architecture, Http Protocol Details, HTTP Parameters, HTTP Messages, HTTP Requests , HTTP Responses, HTTP Response Codes 1xx,2xx,3xx,4xx,5xx etc, HTTP Methods, GET,HEAD,POST,PUT,DELETE,CONNECT,OPTIONS,TRACE,HTTP Status Codes ,HTTP Header Fields, HTTP Security, HTTPS Protocol ,Basic Working of HTTPS Basics, Encoding and Decoding, Same Origin Policy (SOP)	Hands-on lab on Web Application
Day13b	**WEB APPLICATION SECURITY -I** Different Types of Web Applications Attacks and Threats, Hacking Methodology, Web Application Hacking Tools, Firewall,WafW00fWeb Application Vulnerabilities & Countermeasures	Hands-on lab on Web Application Security and its Countermeasures
Day14	**WEB APPLICATION SECURITY -II** Apache Web Server Concepts, Web Server Attacks, Web Server Attacks Methodology, Web Server Attack Tools, Countermeasures, Patch Management, Web Server Security Tools, Web Server Pen Testing Countermeasures, Web Application Security Testing Tools, Vulnerability Scanning, Acunetix & W3af,Nikto,WAF Testing, WAF	Hands on lab on Web Application Security and its Countermeasures.
Day15	**WEB APPLICATION SECURITY -III** Brute Force Attack in Web Application, Command Injection in Web Application, SQL Injection in Web Application, XSS Reflected in Web Application, XSS Store in Web Application	Hands on lab on Web Application Security and its Countermeasures.
Day16	**NETWORK TRAFFIC ENCRYPTION USING IPSec** IP Security, Protocols used in IPSec, Security Architecture of IPSec and Modes of IPSec, VPN, Types of VPN,IP Security, Protocols used in IPSec, SSH Port Forwarding	Hands-on lab on configuring IP Security between 02 Hosts.
Day17	**INTRUSION DETECTION SYSTEM USING SNORT IDS** Introduction to IDS, Types of IDS, Introduction to IDS, , Architecture of Snort, Logical components of snort, Placement of Snort, Component used in Snort, Implementation Functions of IDS, Rules in snort Tools Of Intrusion Detection, Rule Actions and Protocols, Detection	Hands-on lab on Installing and configuring IDS.
Day18	**NETWORK SECURITY-I** Introduction to Network Security, Introduction to MAC address, Introduction to CAM Table, Layer 2 Attacks, Spanning Tree Protocol (STP) Attacks, Preventing STP Manipulation Attacks, Address Resolution Protocol (ARP) Attacks, Media Access Control, Content Addressable Memory (CAM) Table Overflow, CAM Flooding Attacks, Cisco Discovery Protocol (CDP) and the Link Layer Discovery Protocol, VLAN(LLDP), VLAN Hopping, VLAN Hopping using Switch Spoofing, VLAN Hopping using Double Tagging, Countermeasures for VLAN Hopping, DHCP Starvation Attacks, DHCP Spoofing Attacks, Switch port	Hands-on lab on preventing CAM Flooding Attacks by using Switch Port Security,

	Security, MAC-Port Binding Types, Switch Port Violations, Switch Port Security, Preventing CAM Flooding Attacks by using Switch Port Security	
Day19	**NETWORK SECURITY-II** Introduction to DHCP, DHCP Spoofing Attack, DHCP Starvation attacks, DHCP Starvation Attack using Yersinia, Countermeasure for DHCP Starvation attack,DHCP Spoofing Attack Scenarios, DHCP Snooping, Preventing unauthorized access to DHCP Server by using DHCP Snooping, DHCP Snooping Configuration Example, IP Source Binding, Preventing MAC Spoofing by using IP Source Binding, Port Mirroring, Configuring Port Mirroring	Hands-on lab on Preventing unauthorized access to DHCP Server by using DHCP Snooping, and IP Source Binding,
Day20	**PENETRATION TESTING USING METASPLOIT** Introduction to Penetration Testing, Penetration testing methodology, Types of penetration testing, Pen Testing Techniques, Penetration Testing Tools, Examples of Free and Commercial Tools, Limitations of Pentest tools. Introduction to Penetration Testing, Penetration testing methodology, Types of penetration testing, Pen Testing Techniques, Penetration Testing Tools, Examples of Free and Commercial Tools, Limitations of Pentest tools. Metasploit GUIs, MSF Community Edition, Armitage Binary Payloads, Client-Side Exploits, Social Engineering Toolkit, Client-side Attack and Privilege Escalation with Meterpreter using Social Engineering Toolkit	Hands-on lab on Penetration Testing using Metasploit