Information Booklet cum Syllabus

Of

Ethical Hacking and Information Security

Revision-I

July 2022

National Institute of Electronics and Information Technology

An Autonomous Scientific Society under

Ministry of Electronics and Information Technology, Government of India

NIELIT Gorakhpur Deoria Road Gorakhpur (U.P.) -273010	NIELIT Extension Centre Lucknow NIELIT Lucknow Sumit Complex, A-1/9, Vibhuti Khand, Gomti Nagar, Lucknow – 226010

CONTENTS

1. About Course

This course provides learners with real practical hands-on learning to gain real-world experience as a penetration tester or an ethical hacker. This course provides a practical hands-on approach and enable the learners to identify the vulnerable areas of the information system and to apply countermeasures against the vulnerabilities.

2. NIELIT

National Institute of Electronics and Information Technology, NIELIT, (Erstwhile DOEACC Society) is an autonomous scientific society of the Ministry of Electronics & Information Technology, Government of India. The Society is registered under the Societies Registration Act, 1860. NIELIT was set up to carry out Human Resource Development and related activities in the area of Information, Electronics & Communications Technology (IECT). NIELIT is engaged both in Formal & Non-Formal Education in the areas of IECT besides development of industry oriented quality education and training programmes in the state-of-the-art areas. NIELIT has endeavored to establish standards to be the country's premier institution for Examination and Certification in the field of IECT. It is also one of the National Examination Body, which accredits institutes/organizations for conducting courses in IT and Electronics in the non-formal sector.

3. Objective of Course

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.

4. Job Roles of Course

After successful completion of the qualification the candidates shall be employed in the industries for following occupations:

- Penetration Tester
- Security Consultant,
- Network Security Specialist
- Site Administrator
- Ethical Hacker

5. Eligibility

Pursuing Diploma /Graduate

6. Total duration of the Course

80 Hours (Theory: 32 Hrs, Practical/Tutorial: 48 Hrs)

7. Course Details

7.1.Course Outline and Objective of Each Unit

S. No.	Unit Name	Duration (Theory) in Hours	Duration (Practical) in Hours	Total Learning Hrs.	Learning Objectives
1.	Network Primer **I**	03	01	04	After successful completion of the module, the students shall be able to • Understand the network concepts and terminologies. • Understand the OSI, TCP/IP Model and OSI PDU Terms • Understand the PDU header formats
2.	Network Primer **II**	02	01	03	After successful completion of the module, the students shall be able to • Understand the concept of IP addressing • Understand subnetting basics, Subnet Masks, Classless Inter-Domain Routing (CIDR).
3.	Network Primer **III**	02	03	05	After successful completion of the module, the students shall be able to • Understand about IANAand RIR, • Understand the TCP/IP Troubleshooting utilities
4.	Exploring NMAP and Wireshark	01	02	03	After successful completion of the module, the students shall be able to • Discover the ports, services running on the host, operating system and version using NMAP tool . • Captures network traffic using Wireshark
5.	Information Gathering	02	03	05	After successful completion of the module, the students shall be able to • Collect the information visible in public domain • Create the security profile of the target entity.
6.	Sniffing, ARP Cache Poisoning & MITM Attacks	01	03	04	After successful completion of the module, the students shall be able to • Understand about different types of Man in the Middle (MITM) Attacks • Understand about Sniffing, ARP Cache Poisoning. • Apply countermeasures against the MITM Attacks
7.	Password Cracking	02	03	05	After successful completion of the module, the students shall be able to • Understand the different types of password attacks . • Assess the password hashes and password strength. • Apply countermeasures against the Password Attacks

8.	IP Spoofing & Denial of Service	01	03	04	After successful completion of the module, the students shall be able to • Understand about different types of Spoofing techniques. • Understand about different types of DoS Attacks • Apply countermeasures against the Spoofing Attacks
9.	Trojan, Backdoor and Virus	01	03	04	After successful completion of the module, the students shall be able to • Understand Types of Virus, Trojans, Backdoor, and Keylogger. • Apply countermeasures against the malicious program .
10.	Steganography	01	02	03	After successful completion of the module, the students shall be able to • Understand different types of Information Hiding Techniques • Understand Steganography, Different methods of Steganography.
11.	E-Mail Spoofing and Phishing	01	02	03	After successful completion of the module, the students shall be able to • Understand concept of Email and its protocol • Understand different types of Phishing-mails. • Understand Sender Policy Framework,(SPF),DKIM and DMARC policy to prevent spoofed and spam mail.
12.	Securing E-Mail Communication	01	02	03	After successful completion of the module, the students shall be able to • Understand about PGP, MIME, S/MIME. • Secure the E-Mail Communication using PGP .
13.	Web Application Primer	01	02	03	After successful completion of the module, the students shall be able to • Understand terminologies of Web applications, working of website, Types of website, Basic Features of HTTP, URI , URL , URN, Cookies, Session, HTTP Architecture.
14.	Web Application Security-I	02	02	04	After successful completion of the module, the students shall be able to • Understand different Types of Web Applications Attacks and Threats, Hacking Methodology, Web Application Hacking tools. • Understand and applying countermeasures against the Web Applications Attacks

15.	Web Application Security-II	01	02	03	After successful completion of the module, the students shall be able to • Understand about Web Server Attacks, Attacks Methodology, Web Server security tools, Vulnerability Scanning • Apply countermeasures against Web Server Attacks
16.	Web Application Security-III	01	02	03	After successful completion of the module, the students shall be able to • Understand about Brute Force Attack in Web Application, Command Injection, SQL Injection in Web Application XSS Reflected in Web Application. • Apply countermeasures against web application Attacks
17.	Network Traffic Encryption	02	02	04	After successful completion of the module, the students shall be able to • Understand IPSec, Protocols used in IPSec, Security Architecture of IPSec and Modes of IPSec, VPN, • Understand SSH Port Forwarding • Secure the Network Communication using IPSec .
18.	Intrusion Detection System	02	03	05	After successful completion of the module, the students shall be able to • Understand about IDS, types of IDS, architecture of Snort • Detect alerts for malicious activity.
19.	Network Security-I	01	02	03	After successful completion of the module, the students shall be able to • Under different types of Layer 2 Attacks • Apply Switch Port security to prevent CAM Flooding attacks..
20.	Network Security-II	01	02	03	After successful completion of the module, the students shall be able to • Understand about Securing DHCP, DHCP Snooping, MAC Spoofing, IP Source Binding, Port Mirroring
21.	Penetration Testing using Metasploit	03	03	06	After successful completion of the module, the students shall be able to • Use methodologies and techniques used to perform penetration testing to test the security of application or system
Total Hours		**32**	**48**	**80**	

7.2.Detaied Syllabus

Unit Name	**Contents**	**Hrs.**

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	04
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	03
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, the Possible Session States in netstat output,getmac,nslookup, DNS Resource Records, Troubleshooting IP Addressing	05
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	03

Information Gathering	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, OSINT Framework, 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.	05
Sniffing, ARP Cache Poisoning & MITM Attacks	Sniffing, ARP Cache Poisoning, Man in the Middle (MITM) Attacks	04
Password Cracking	Password Hashes, Password Cracking types, Dictionary Attack, Brute Force Attacks, Cracking Passwords using John the Ripper, Other password Cracking tools, How passwords are stored in Linux,/etc/passwd and /etc/shadow,How passwords are stored in Windows, Testing SSH Password and Hardening of SSH,Password Cracking Countermeasures	05
IP Spoofing & Denial of Service	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	04
Trojan, Backdoor and Virus	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	04
Steganography	Information Hiding, Techniques Steganography, Steganography with CMD, Steganography using image file Steghide tool, Scapy tool used for Steganography, ICMP, Steganography using ICMP Payload Scapy tool used for Steganography	03
E-Mail Spoofing and Phishing	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	03
Securing E-Mail Communication	PGP, E-mail Security, Securing E-Mail Communication, PGP, MIME, S/MIME, Difference between PGP and S/MIME, Scenario For E-mail Security	03
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, HTTP Status Codes ,HTTP Header	03

	Fields.	
Web Application Security –I	Different Types of Web Applications Attacks and Threats, Hacking Methodology, Web Application Hacking Tools, Firewall,WafW00fWeb Application Vulnerabilities & Countermeasures	04
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	03
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	03
Network Traffic Encryption	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	04
Intrusion Detection System	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	05
Network Security-I	Introduction to Network Security , Introduction to MAC address, Introduction to CAM Table, CAM Flooding Attacks , Introduction to Macof tool, MAC-Port Binding Types, Switch Port Violations, Switch Port Security, Preventing CAM Flooding Attacks by using Switch Port Security	03
Network Security-II	Securing DHCP, DHCP Snooping, Preventing unauthorized access to DHCP Server by using DHCP Snooping, MAC Spoofing, IP Source Binding, Preventing MAC Spoofing by using IP Source Binding, Port Mirroring	03
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, ArmitageBinary Payloads, Client-Side Exploits, Social Engineering Toolkit, Client-side Attack and Privilege Escalation with Meterpreter using Social Engineering Toolkit	06
Total Hours		80

8. Reference Books/Study Material

a. The Basics of Hacking and Penetration Testing, Patrick Engebretson 2nd edition Syngress.
b. Ethical Hacking A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking, By Hilary Morrison, hein smith · 2018, CreateSpace Independent Publishing Platform
c. Hands-on Penetration Testing for Web Applications,2022, Richa Gupta, BPB
d. Ethical Hacker's Penetration Testing Guide, 2022, Samir Kumar Rakshit, BPB

9. Practical Assignments

Assignment-1. Studying different LAN media and Cabling.
Assignment-2. Verifying MTU of Network interface and Changing the MTU size in OS
Assignment-3. Practice on IP Subnetting on CLASS A, B & C networks.
Assignment-4. Hands-on lab on Nslookup ,TCP/IP Utilities, hostname, Arp, Ping, tracert / traceroute, Netstat, Getmac, Nslookup
Assignment-5. Hands-on lab on scanning using NMAP.
Assignment-6. Hands-on lab on traffic capturing using Wireshark
Assignment-7. Hands-on lab on Information Gathering, OSINT tools, Scanning, Whois, nslookup and its countermeasures
Assignment-8. Hands-on Lab on Sniffing, ARP Cache Poisoning, Man in the Middle (MITM) Attacks using ettercap & its Countermeasures
Assignment-9. Hands-on lab on Password cracking techniques, Password Testing With Hydra, exploring, /etc/passwd and /etc/shadow and its countermeasures
Assignment-10. Hands-on lab on IP Spoofing, Denial of Service (DoS) ,hping, netstat, and its countermeasures
Assignment-11. Hands-on lab on Steganography CMD and using an image file Steganography using ICMP Payload
Assignment-12. Hands-on lab on demonstration on phishing mail and its countermeasures.
Assignment-13. Hands-on lab on demonstration on SPF ,DKIM and DMARC .
Assignment-14. Hands-on lab on Web Application Primer
Assignment-15. Hands-on lab on Web Application Security and its Countermeasures
Assignment-16. Hands-on lab on Web Application Security and its Countermeasures.
Assignment-17. Hands-on lab on configuring IPSec between 02 Hosts.
Assignment-18. Hands-on lab on Installing and configuring IDS.
Assignment-19. Hands-on lab on preventing CAM Flooding Attacks by using Switch Port Security
Assignment-20. Hands-on lab on Preventing unauthorized access to DHCP Server by using DHCP Snooping, and IP Source Binding,
Assignment-21. Hands-on lab on Penetration Testing using Metasploit