

DIPLOMA PROGRAM
INFORMATION SECURITY AND ETHICAL HACKING (Version 7.0)
Detailed Course Curriculum (2012-2013)
For details visit www.eikontech.net

MODULE: INTRODUCTION TO INFORMATION SECURITY AND ETHICAL HACKING

- INFORMATION SECURITY AND HACKING COMBO
- ESSENTIAL TERMINOLOGIES
- SECURITY AND ITS NEED
- WHY IS IT SECURITY NECESSARY?
- IT SECURITY SERVICES LIFE CYCLE
- OPERATING SYSTEM BASICS
- DATA COMMUNICATION BASICS
- BASICS OF COMPUTER NETWORKING
- OSI AND TCP/IP MODEL
- TCP VS UDP
- TCP FRAME STRUCTURE
- UDP FRAME STRUCTURE
- TCP COMMUNICATION FLAGS
- NETWORKING DEVICES
- CYBER THREATS AND ISSUES
- AN APPROACH TOWARDS HACKING
- PROTECTING YOUR COMPUTER AND NETWORK
- SOFTWARE SECURITY FOR PORTABLE COMPUTERS
- DEFENDING AGAINST SOCIAL ENGINEERS AND PHISHERS
- PROTECTING YOUR PASSWORD AND LOGGING ON SECURELY
- HOW PASSWORDS GET CRACKED
- TOP 4 METHODS TO HACK FACEBOOK PASSWORD WITHIN 5 MIN
- SELECTING TOOLS
- SAFETY RULES

MODULE: DESKTOP AND SERVER SECURITY

UNIT 1: DESKTOP AND SERVER SECURITY

- INTRODUCTION
- SECURING YOUR MIGRATED WINDOWS 7 DESKTOP
- DESKTOPS: LOCAL RIGHTS AND PRIVILEGES
- OVERALL DESKTOP SECURITY
- WHAT IS REGISTRY?
- REGISTRY EDITING
- BACKUPS AND RECOVERY
- POLICY
- WINDOWS 9X OPERATING SYSTEMS
- STEPS TO CREATE REGISTRY VALUES

- SOME OF THE EXAMPLES TO CHANGE THE REGISTRY DEFAULT SETTINGS
- NT SECURITY
- THE LOGON PROCESS
- SECURITY ARCHITECTURE COMPONENTS
- INTRODUCTION TO SECURING IN NT BOX
- BACKUPS
- WINDOWS VULNERABILITIES AND THREATS
- DETERMINING IF YOU ARE ACTIVELY BEING COMPROMISED
- CLIENT –SERVER ARCHITECTURE
- SERVER SECURITY PRINCIPLES
- SECURING THE SERVER OPERATING SYSTEM
- APPLICATIONS AND NETWORK PROTOCOLS
- CONFIGURE OS USER AUTHENTICATION
- WINDOWS 8 INTRODUCTION AND SECURITY

UNIT 2: LINUX SECURITY

- INTRODUCTION
- BENEFITS OF LINUX
- HOW SECURE SHOULD MY LINUX BE?
- LAYERS OF LINUX/UNIX
- LINUX DIRECTORY STRUCTURE (FILE SYSTEM STRUCTURE) EXPLAINED WITH EXAMPLES
- WHY SHADOW YOUR PASSWORD FILE?
- WHAT IF UNSHADOW PASSWORD?
- HOW TO SET UP A FIREWALL UNDER LINUX?
- SECURING AND HARDENING TIPS LINUX SYSTEMS
- WINDOWS VS. LINUX DESIGN
- REALISTIC SECURITY AND SEVERITY METRICS
- CERT VULNERABILITY NOTES DATABASE RESULTS

MODULE: DATA SECURITY

UNIT1: DATA SECURITY

- INTRODUCTION
- DATA SECURITY MANAGEMENT
- CHARACTERISTICS OF ACCESS SECURITY IN THE SYSTEM
- DATA SECURITY ISSUES AND SOLUTIONS
- INTRODUCTION TO CLOUD COMPUTING
- PROTECTING THE USERS
- CLOUD COMPUTING IN REAL DOMAIN
- BENEFITS FROM CLOUD COMPUTING

UNIT 2: DATA BACKUP

- DATA BACKUP
- INTRODUCTION
- DATA BACKUP STRATEGIES
- OFFLINE DATA BACKUP

- ONLINE DATA BACKUP

UNIT 3: CRYPTOGRAPHY

- STRENGTH OF THE CRYPTOGRAPHY
- GOALS OF CRYPTOGRAPHY
- SOME TECHNICAL TERMS
- TYPES OF CIPHER TEXT
- TYPES OF CRYPTOGRAPHY
- DATA ENCRYPTION STANDARD (DES)
- IDEA: INTERNATIONAL DATA ENCRYPTION ALGORITHM
- ASYMMETRIC CRYPTOGRAPHY
- RSA ALGORITHM
- HASH FUNCTIONS
- DIGITAL SIGNATURES
- DIGITAL CERTIFICATION

UNIT 4: STEANOGRAPHY

- HOW DOES IT WORK?
- STEGANOGRAPHY IN IMAGES
- STEGANOGRAPHY IN AUDIO
- GENETIC ALGORITHM APPROACH
- STEGANOGRAPHY IN VIDEO

MODULE: NETWORK SECURITY

UNIT 1: MOBILE SECURITY

- INTRODUCTION
- WHAT IS MOBILE?
- ARCHITECTURE OF MOBILE COMMUNICATION
- MOBILE GENERATION
- TECHNOLOGY OF MOBILE COMMUNICATION
- MOBILE PHONE STANDARDS
- PROTOCOLS USED IN MOBILE
- INTRODUCTION TO SMS MESSAGING
- SIM
- INTRODUCTION TO MOBILE OS
- POPULAR OPERATING SYSTEMS
- BLACKBERRY OS FROM RIM
- IOS FROM APPLE INC
- SYMBIAN OS
- WINDOWS PHONE OS
- SAMSUNG BADA
- WHAT IS NFC, HOW IT WORKS AND WHAT ARE ITS PRACTICAL APPLICATIONS
- WHY IS MOBILE SECURITY IMPORTANT?
- MOBILE PLATFORM COMPARISON
- MOBILE THREATS

- TRENDS OF MOBILE THREATS
- WHAT IS BLUETOOTH? & HOW DOES IT WORK??
- HOW BLUETOOTH CREATES A CONNECTION
- BLUETOOTH ATTACKS ON MOBILE PHONES
- BLUETOOTH WEAKNESSES
- MOBILE SAFEGUARDS AND SOLUTIONS

UNIT 2: VOICE OVER INTERNET PROTOCOL

- DEFINITION & TRENDS
- SERVICES
- TYPES OF VOIP
- COMPONENTS OF VOIP
- IP TELEPHONY & IP PAGING
- PROTOCOLS AND ACRONYMS
- REASONS FOR VOIP
- PROBLEMS IN VOIP
- SKYPE
- VOIP SECURITY SCENARIO
- HOW DO WE SECURE VOIP?

UNIT 3: VIRTUAL PRIVATE NETWORK SECURITY

- INTRODUCTION TO VPN
- APPLICATION & REQUIREMENTS OF VPN
- VPN TYPES
- OPEN VPN
- MODELS OF VPN
- IPSEC VPN
- VPN SECURITY FRAMEWORK
- VPN SECURITY ISSUES
- OTHER VPN THREATS

UNIT 4: WIRELESS LAN

- INTRODUCTION
- 802.11 STANDARDS OF WLAN
- BASICS OF WIRELESS LAN
- ANTENNAS
- ACCESS POINT POSITIONING
- ROGUE ACCESS POINT
- WIRED EQUIVALENT PRIVACY
- DOS ATTACK
- MAN IN MIDDLE ATTACK (MITM)
- COUNTERMEASURES FOR WLAN
- TOOLS
- WIRELESS INTRUSION DETECTION
- OPEN SOURCE SCANNING SOFTWARE

UNIT 5: ROUTER SECURITY

- WHAT IS A ROUTER?
- STATIC AND DYNAMIC ROUTING
- WORK TO ROUTER
- KEEPING THE MESSAGES MOVING
- DIRECTING TRAFFIC
- TRANSMITTING PACKETS
- KNOWING WHERE TO SEND DATA
- MAC ADDRESSES
- UNDERSTANDING THE PROTOCOLS
- TRACING THE MESSAGE
- DENIAL OF SERVICE ATTACK
- CONFIGURATION OF ROUTER
- PROTOCOLS ON A ROUTER
- RFC 1483
- HANDSHAKE PROTOCOLS
- NAT (NETWORK ADDRESS TRANSLATION)
- NAPT SERVICES
- ADSL DETAILS
- TROUBLE SHOOTING
- ROUTING TABLE PROBLEMS
- VARIOUS TYPES OF ATTACKS
- SECURING THE ROUTERS

UNIT 6: INTRUSION DETECTION AND PREVENTION

- INTRODUCTION
- INTRUSION
- DETECTION AND PREVENTION
- IDS
- NEED OF IDS
- COMPONENTS
- TYPES
- WHAT IS NOT AN IDS?
- DETECTION METHODOLOGIES
- VARIOUS TOOLS AVAILABLE
- LIMITATIONS OF IDS
- INTRUSION PREVENTION SYSTEM
- TYPES
- NETWORK BASED IPS
- COUNTER MEASURES TAKEN BY AN IPS
- RISKS INVOLVE

UNIT 7: ACCESS CONTROL SYSTEM

- INTRODUCTION: WHAT IS ACCESS CONTROL
- ACCESS CONTROL IN PHYSICAL SECURITY
- ACCESS CONTROL IN INFORMATION SECURITY
- NEED OF AN ACCESS CONTROL SYSTEM
- SOME CONCEPTS RELATED TO ACCESS CONTROL
- POLICIES, MODELS, AND MECHANISMS
- ACCESS CONTROL TECHNIQUES
- NON-DISCRETIONARY ACCESS CONTROL
- MANDATORY ACCESS CONTROL (MAC)
- ROLE-BASED ACCESS CONTROL
- LATTICE BASED ACCESS CONTROL
- TEMPORAL CONSTRAINTS
- WORKFLOW
- CHINESE WALL
- ACCESS CONTROL MODELS
- ACCESS CONTROL MANAGEMENT INTRODUCTION

MODULE: WEB SECURITY

UNIT 1: LAN SECURITY

- THE INITIAL INTERNETTING CONCEPTS
- INTRODUCTION TO LAN
- WHY LAN SECURITY IS IMPORTANT
- LAN/WAN COMPONENTS
- TOPOLOGY
- PROTOCOLS
- THREATS OF LAN
- INAPPROPRIATE ACCESS TO LAN RESOURCES
- DISCLOSURE OF DATA
- UNAUTHORIZED MODIFICATION OF DATA AND SOFTWARE
- DISCLOSURE OF LAN TRAFFIC
- SPOOFING OF LAN TRAFFIC
- DISRUPTION OF LAN FUNCTIONS
- SECURITY SERVICES AND MECHANISMS
- HACKING MAC ADDRESS
- NETWORK SCANNERS
- TYPES OF SCANNING
- SCANNING METHODOLOGY

UNIT 2: FIREWALL SECURITY

- FIREWALLS
- WORKING OF FIREWALL
- TYPES OF FIREWALL
- PROXY SERVER
- WHY PROXYING?

- WORKING OF PROXY SERVER
- ADVANTAGES OF PROXYING
- DISADVANTAGE OF PROXYING
- APPLICATIONS OF FIREWALL

UNIT 3: INTERNET SECURITY

- INTRODUCTION
- SECURITY ATTACKS AND SECURITY PROPERTIES
- THREATS FACED ON INTERNET
- INTRODUCTION TO IP ADDRESSES
- FINDING IP ADDRESS OF A REMOTE SYSTEM
- HIDING YOUR IDENTITY: ANONYMOUS SURFING
- PROXIES SERVERS
- WHAT IS A SOCKS PROXY SERVER?

UNIT 4: E-MAIL SECURITY

- INTRODUCTION
- HISTORY OF E-MAIL
- EMAIL ADDRESSES
- HOW E-MAIL WORKS?
- VARIOUS MAIL SERVERS
- E-MAIL PROTOCOLS
- ANALYSIS OF EMAIL HEADERS
- EMAIL TRACKING
- IP TRACKING USING EMAIL
- SPAMMING
- WAYS TO PREVENT SPAM
- SECURITY THREATS TO YOUR EMAIL COMMUNICATIONS
- SETUP EMAIL FILTER IN GMAIL, HOTMAIL & YAHOO
- HOW TO STEAL DATA FROM AN E-MAIL?
- E-MAIL EXCHANGE SERVER SECURITY
- VIRUS PROTECTION
- RPC OVER HTTP
- PROTECTING FRONT-END SERVERS
- KEEP EXCHANGE SERVER UP-TO-DATE
- CYBER LAWS REGARDING SPAMMING
- SECURITY POLICIES

MODULE: VAPT

UNIT 1:

- INTRODUCTION
- IMPORTANT TECHNICAL TERMS
- INFORMATION GATHERING
- SCANNING AND FINGERPRINTING

UNIT 2: VULNERABILITY ASSESSMENT

- VULNERABILITIES
- VULNERABILITY ASSESSMENT
- PROTECTIVE MEASURES
- GENERAL APPROACH
- FOOTPRINTING
- VULNERABILITY ASSESSMENT: THE RIGHT TOOLS TO PROTECT YOUR CRITICAL DATA
- TYPES OF VULNERABILITY ASSESSMENT
- THE CHALLENGES OF VULNERABILITY ASSESSMENTS
- TOOLS FOR VA
- NETWORK SECURITY AUDIT CASE STUDY

UNIT 3: PENETRATION TESTING

- INTRODUCTION AND METHODOLOGY
- TYPES OF PENETRATION TESTS
- METHODOLOGY
- PENETRATION TESTING APPROACH
- PENETRATION TESTING VS VULNERABILITY ASSESSMENT
- HOW VULNERABILITIES ARE IDENTIFIED
- A SAMPLE PENETRATION TESTING REPORT
- SECURITY SERVICES
- SECURITY SERVICES MANAGEMENT TOOLS
- FIREWALL
- AUTOMATED VULNERABILITY SCANNING
- AN APPROACH TO VULNERABILITY SCANNING
- PASSWORD CRACKING AND BRUTE FORCING
- DENIAL OF SERVICE (DOS) TESTING
- PENETRATION TESTING TOOLS
- ESCALATION OF PRIVILEGES
- CASE STUDIES

MODULE: HACKING ATTACKS

UNIT 1: MALWARES

- INTRODUCTION TO MALWARES
- MALWARE DETECTION TECHNIQUES
- COUNTER MEASURES TYPES OF MALWARES
- INSTALLING BOTS ON TARGET MACHINES
- ATTACKING METHODS
- WORKING OF BOTS

UNIT 2: HACKING ATTACKS

- INTRODUCTION TO ATTACKS
- TYPES OF ATTACKS
- NON-TECHNICAL ATTACK

- TABNABBING: A NEW TYPE OF PHISHING ATTACK
- TECHNICAL ATTACKS
- PASSWORD ATTACKS
- BACKTRACK
- BACKDOOR
- ROOTKITS
- MALWARE GLOSSARY

UNIT 3: ART OF GOOGLING

- INTRODUCTION
- THE GOOGLE TOOLBAR
- SEARCHING TECHNIQUES
- DIRECTORY LISTING
- LOCATING CGI-BIN
- LOCATING ROBOTS.TXT
- CAMERA HACKING
- SOME TRICKS
- THE HARVESTER TOOL
- ARTICLES

MODULE: INFORMATION SECURITY MANAGEMENT SYSTEM

UNIT 1: SECURITY AUDITING

- INTRODUCTION
- BACKGROUND
- SECURITY AUDITING OBJECTIVES
- RISK INVOLVED
- AUDITING STEPS

UNIT 2: LEAD AUDITOR: IT (LA-27001

- INFORMATION SECURITY AND MANAGEMENT SYSTEM
- CRITICAL CONTROL: INCIDENT RESPONSE CAPABILITY
- CRITICAL CONTROL: SECURITY SKILLS ASSESSMENT AND APPROPRIATE TRAINING TO FILL GAPS
- CRITICAL CONTROL: DATA LOSS PREVENTION
- CRITICAL CONTROL 14: WIRELESS DEVICE CONTROL
- MANAGING SECURITY AWARENESS
- RISK ASSESSMENT, BUSINESS CONTINUITY AND DISASTER
- SECURITY MANAGEMENT PRACTICES AND FRAMEWORK

MODULE: CYBER LAWS AND IT ACTS

- INTRODUCTION
- CYBER LAWS: INTERNATIONAL PERSPECTIVE
- E-GOVERNANCE
- IMPEDIMENTS IN IMPLEMENTING E-GOVERNANCE PROJECTS FROM LEGAL PERSPECTIVE
- ANALYSIS OF PROBLEMS – REPERCUSSIONS
- RELEVANT LAWS

- JURISPRUDENCE OF INDIAN CYBER LAW
- THE INFORMATION TECHNOLOGY ACT, 2000 (SOME LAWS)
- AMENDMENT TO THE IT ACT 2000 BY ITAA2008
- ADVANTAGES OF CYBER LAWS
- PROSECUTION OF CYBER CRIMES UNDER INDIAN CYBER LAWS (IT ACT, 2000)
- PROBABLE SOLUTIONS
- ARTICLES ON CYBER LAWS
- CASES ON CYBER LAWS

MODULE : CYBER FORENSICS

UNIT 1: CYBER CRIME

- INTRODUCTION TO CYBER FORENSICS
- FORENSICS PROCEDURES
- HISTORY OF COMPUTER FORENSICS
- CYBER SECURITY & FORENSICS
- WHAT IS CYBER CRIMES?
- CLASSIFICATION OF CYBER CRIME
- WHY LEARN ABOUT CYBER CRIME
- TYPES OF CYBER CRIME
- CHARACTERISTICS OF COMPUTER CRIME
- PREVENTION OF CYBER CRIME
- QUESTIONNAIRE BASED ON RECOMMENDATIONS FROM THE FOURTH MEETING OF GOVERNMENTAL EXPERTS ON CYBER-CRIME CYBER CRIMINALS
- MODE AND MANNER OF COMMITTING CYBER CRIME
- UNDERSTAND THE FUNDAMENTALS

UNIT 2: CYBER FORENSICS

- CYBER FORENSICS: DETAILED VIEW
- DIGITAL EVIDENCE
- CHALLENGES OF FORENSIC SCIENCE
- FORENSIC METHODOLOGY
- SOME FORENSIC SOFTWARES/ HARDWARES
- BASIC APPROACHES
- FORENSICS TOOLS EXAMPLE

UNIT 3: CATCHING CRIMINALS

- CYBER TERRORISM- THE DARK SIDE OF THE WEB WORLD
- HONEY POTS

UNIT 4: MOBILE FORENSICS

- INTRODUCTION TO MOBILE FORENSICS
- GENERAL PHONES (NOKIA, SAMSUNG, LG)
- BLACKBERRY DEVICES
- CHINESE DEVICES
- EXTRACTION METHODS OF MOBILE FORENSICS
- MOBILE PHONE CHARACTERISTICS

- MOBILE FORENSIC ANALYSIS
- THE CHALLENGES OF MOBILE FORENSICS
- TOOLS FOR MOBILE FORENSICS
- FORENSIC TOOLKIT
- CHECKLIST OF TOOLS FOR CYBER FORENSICS