FRONT RUNNER DIPLOMA PROGRAM
INFORMATION SECURITY & ETHICAL HACKING

Detailed Course Curriculum (2012-2013)

MODULE: Introduction to Information Security and Ethical Hacking

1.1 INFORMATION SECURITY AND HACKING COMBO
1.2 ESSENTIAL TERMINOLOGIES
1.3 SECURITY AND ITS NEED
1.4 WHY IS IT SECURITY NECESSARY?
1.5 IT SECURITY SERVICES LIFE CYCLE
1.6 OPERATING SYSTEM BASICS
1.7 DATA COMMUNICATION BASICS
1.8 BASICS OF COMPUTER NETWORKING
1.9 OSI AND TCP/IP MODEL
1.10 NETWORKING DEVICES
1.11 CYBER THREATS AND ISSUES
1.12 AN APPROACH TOWARDS HACKING
1.13 PROTECTING YOUR COMPUTER AND NETWORK
1.14 SOFTWARE SECURITY FOR PORTABLE COMPUTERS
1.15 DEFENDING AGAINST SOCIAL ENGINEERS AND PHISHERS
1.16 PROTECTING YOUR PASSWORD AND LOGGING ON SECURELY
1.17 SELECTING TOOLS
1.18 SAFETY RULES

H.A LINKS SOLUTION

appin
The Information Security Specialist

MODULE: Desktop and Server Security

UNIT 1: DESKTOP & SERVER SECURITY

1.1 INTRODUCTION
1.2 WHAT IS REGISTRY?
1.3 REGISTRY EDITING
1.4 BACKUPS AND RECOVERY
1.5 POLICY
1.6 .INI FILE VIRTUALIZATION
1.7 WINDOWS 9X OPERATING SYSTEMS
1.8 STEPS TO CREATE REGISTRY VALUES
1.9 SOME OF THE EXAMPLES TO CHANGE THE REGISTRY DEFAULT SETTINGS
1.10 NT SECURITY
1.11 SECURITY ARCHITECTURE COMPONENTS
1.12 INTRODUCTION TO SECURING IN NT BOX
1.13 BACKUPS
1.14 WINDOWS VULNERABILITIES AND THREATS
1.15 HOW TO DETERMINE IF YOU ARE AT RISK? USE ANY VULNERABILITY SCANNER
1.16 HOW TO PROTECT AGAINST THE WINDOWS SERVICES VULNERABILITIES

UNIT 2: LINUX SECURITY

2.1 INTRODUCTION: LINUX BASED
2.2 BENEFITS OF LINUX
2.3 HOW SECURE SHOULD MY LINUX BE?
2.4 HOW TO SET UP A FIREWALL UNDER LINUX?
2.5 WINDOWS VS. LINUX DESIGN
2.6 REALISTIC SECURITY AND SEVERITY METRICS
2.7 CERT VULNERABILITY NOTES DATABASE RESULTS

H.A LINKS SOLUTION

appin
The Information Security Specialist

MODULE: Web Security

UNIT 1: NETWORK AND NETWORKING CONCEPT

1.1 AN INTRODUCTION TO NETWORKING
1.2 NETWORKING STANDARD AND THE OSI MODEL
1.3 TRANSMISSION BASICS AND NETWORKING MEDIA
1.4 NETWORK PROTOCOLS & NETWORKING HARDWARE
1.5 TOPOLOGIES AND ACCESS METHODS
1.6 WAN's, INTERNET ACCESS, AND REMOTE CONNECTIVITY
1.7 TCP/IP NETWORKING & FUNDAMENTAL
1.8 TROUBLESHOOTING NETWORK PROBLEMS
1.9 ENSURING INTEGRITY AND AVAILABLITY

UNIT 2: LAN SECURITY

2.1 THREATS OF LAN
2.2 INAPPROPRIATE ACCESS TO LAN RESOURCES
2.3 DISCLOSURE OF DATA
2.4 UNAUTHORIZED MODIFICATION OF DATA AND SOFTWARE
2.5 DISCLOSURE OF LAN TRAFFIC
2.6 SPOOFING OF LAN TRAFFIC
2.7 DISRUPTION OF LAN FUNCTIONS
2.8 SECURITY SERVICES AND MECHANISMS
2.9 HACKING MAC ADDRESS
2.10 NETWORK SECURITY
2.11 IMPLEMENTING AND MANAGING NETWORK

UNIT 3: FIREWALL SECURITY

3.1 FIREWALLS
3.2 WORKING OF FIREWALL
3.3 TYPES OF FIREWALL
3.4 PROXY SERVER
3.5 WHY PROXYING?
3.6 WORKING OF PROXY SERVER
3.7 ADVANTAGES OF PROXYING
3.8 DISADVANTAGE OF PROXYING

H.A LINKS SOLUTION

appin
The Information Security Specialist

MODULE: VAPT

UNIT 1: INTRODUCTION

1.1 IMPORTANT TECHNICAL TERMS
1.2 INFORMATION GATHERING
1.3 SCANNING AND FINGERPRINTING

UNIT 2: VULNERABILITY ASSESSMENT

2.1 VULNERABILITIES
2.2 VULNERABILITY ASSESSMENT
2.3 APPROACHES TO DATA SECURITY
2.4 PROTECTIVE MEASURES
2.5 GENERAL APPROACH
2.6 FOOTPRINTING
2.7 VULNERABILITY ASSESSMENT: THE RIGHT TOOLS TO PROTECT YOUR CRITICAL DATA
2.8 TYPES OF VULNERABILITY ASSESSMENT
2.9 THE CHALLENGES OF VULNERABILITY ASSESSMENTS
2.10 APPIN TOOL FOR VULNERABILITY ASSESSMENT
2.11 TOOLS FOR VA

UNIT 3: PENETRATION TESTING

3.1 INTRODUCTION AND METHODOLOGY
3.2 TYPES OF PENETRATION TESTS
3.3 METHODOLOGY
3.4 PENETRATION TESTING APPROACH
3.5 PENETRATION TESTING VS. VULNERABILITY ASSESSMENT
3.6 HOW VULNERABILITIES ARE IDENTIFIED
3.7 A SAMPLE PENETRATION TESTING REPORT
3.8 SECURITY SERVICES
3.9 SECURITY SERVICES MANAGEMENT TOOLS
3.10 FIREWALL
3.11 AUTOMATED VULNERABILITY SCANNING
3.12 AN APPROACH TO VULNERABILITY SCANNING
3.13 PASSWORD CRACKING AND BRUTE FORCING
3.14 DENIAL OF SERVICE (DOS) TESTING

3.15 PENETRATION TESTING TOOLS
3.16 ESCALATION OF PRIVILEGES

UNIT 4: ENUMERATION

4.1 WHAT IS ENUMERATION
4.2 TECHNIQUES FOR ENUMERATION
4.3 NETBIOS ENUMERATION
4.4 NETBIOS ENUMERATION TOOL: SUPER SCAN
4.5 NetBIOS ENUMERATION TOOL: NetBIOS ENUMERATION
4.6 ENUMERATING USER ACCOUNTS
4.7 ENUMERATE SYSTEM USING DEFUALT PASSWORDS
4.8 SMTP ENUMERATION :-
4.9 SMTP ENUMERATION TOOL: NetSCAN TOOL PRO

UNIT 5: SCANNING NETWORKS

5.1 NETWORK SCANNING
5.2 TYPES OF SCANNING
5.3 CHECKING FOR LIVE SYSTEMS – ICMP SCANNING
5.4 THREE WAY HANDSHAKE
5.5 TCP COMMUNICATION FLAGS
5.6 CREATE CUSTOM PACKET USING TCP FLAGS
5.7 SCANNING TEHCNIQUES
5.8 IP FRAGMENATATION TOOLS
5.9 VULNERABLITY SCANNING TOOLS
5.10 SCANNING COUNTERMEASURES
5.11 WHAT IS Operating System FINGERPRINTING
5.12 ACTIVE BANNER GRABBING USING TELNET

UNIT 6: FOOTPRITING AND RECONNAISSANCES

6.1 FOOTPRINTING TEMINOLOGIES
6.2 WHAT IS FOOTPRINTING
6.3 OBJECTIVES OF FOOTPRINTING
6.4 FOOTPRINTING THREATS
6.5 FINDING A COMPANY'S URLs
6.6 PUBLIC AND RESTRICTED WEBSITES

6.7 SEARCH FOR COMPANY's INFORMATION
6.8 TOOLS TO EXTRACT COMPANY's DATA
6.9 FOOTPRINTING THROUGH SEARCH ENGINES
6.10 COLLECT LOCATION INFORMATION
6.11 SATELLITE PICTURE OF A RESIDENCE
6.12 PEOPLE SEARCH
- PEOPLE SEARCH USING http://pipl.com
- PEOPLE SEARCH ONLINE SERVICES
- PEOPLE SEARCH ON SOCIAL NETWORKING SERVICES

6.13 GATHER INFORMATION FROM FINANCIAL SERVICES
6.14 FOOTPRINTING THROUGH JOB SITES
6.15 MONITORING TARGET USING ALERTS
6.16 COMPETITIVE INTELLIGENCE GATHERING

6.17 WHOIS Lookup
- WHOIS Lookup Result Analysis
- WHOIS Lookup Tools
- WHOIS Lookup online Tools

6.18 Extracting DNS Information
- DNS Interrogation Tools
- DNS Interrogation Online Tools

6.19 Locate the Network Range
6.20 Traceroute
- Traceroute Analysis
- Traceroute Tools

6.21 Mirroring Entire Website Mirroring Tools Mirroring Entire Website Tools

MODULE: Network Security

UNIT 1: MOBILE SECURITY

1.1 INTRODUCTION
1.2 WHAT IS MOBILE?
1.3 ARCHITECTURE OF MOBILE COMMUNICATION
1.4 MOBILE GENERATION
1.5 TECHNOLOGY OF MOBILE COMMUNICATION
1.6 MOBILE PHONE STANDARDS
1.7 PROTOCOLS USED IN MOBILE
1.8 SIM
1.9 MOBILE SAFEGUARDS AND SOLUTIONS

UNIT 2: VO

2.3 TYPES OF VOIP
2.4 COMPONENTS OF VOIP
2.5 IP TELEPHONY & IP PAGING
2.6 PROTOCOLS AND ACRONYMS
2.7 REASONS FOR VOIP
2.8 PROBLEMS IN VOIP

UNIT 3: VIRTUAL PRIVATE NETWORK SECURITY

3.1 INTRODUCTION TO VPN
3.2 APPLICATION & REQUIREMENTS OF VPN
3.3 VPN TYPES
3.4 OPEN VPN
3.5 MODELS OF VPN
3.6 IPSEC VPN
3.7 VPN SECURITY FRAMEWORK
3.8 VPN SECURITY ISSUES
3.9 OTHER VPN THREATS

UNIT 4: WIRELESS LAN

4.1 INTRODUCTION
4.2 BASICS OF WIRELESS LAN
4.3 ANTENNAS
4.4 ACCESS POINT POSITIONING
4.5 ROGUE ACCESS POINT
4.6 WIRED EQUIVALENT PRIVACY
4.7 DOS ATTACK
4.8 MAN IN MIDDLE ATTACK (MITM)
4.9 TOOLS
4.10 WIRELESS INTRUSION DETECTION
4.11 OPEN SOURCE SCANNING SOFTWARE

UNIT 5 : ROUTER SECURITY

5.1 WHAT IS A ROUTER?
5.2 STATIC AND DYNAMIC ROUTING
5.3 WORKS TO ROUTER
5.4 KEEPING THE MESSAGES MOVING
5.5 DIRECTING TRAFFIC
5.6 TRANSMITTING PACKETS
5.7 KNOWING WHERE TO SEND DATA
5.8 MAC ADDRESSES
5.9 UNDERSTANDING THE PROTOCOLS
5.10 TRACING THE MESSAGE
5.11 DENIAL OF SERVICE ATTACK
5.12 CONFIGURATION OF ROUTER
5.13 PROTOCOLS ON A ROUTER
5.14 RFC 1483
5.15 HANDSHAKE PROTOCOLS
5.16 NAT (NETWORK ADDRESS TRANSLATION)
5.17 NAPT SERVICES
5.18 ADSL DETAILS
5.19 TROUBLE SHOOTING
5.20 ROUTING TABLE PROBLEMS
5.21 VARIOUS TYPES OF ATTACKS

5.22 SECURING THE ROUTERS

UNIT 6 INTRUSION DETECTION AND PREVENTION

6.1 INTRODUCTION
6.2 INTRUSION
6.3 DETECTION AND PREVENTION
6.4 IDS
6.5 NEED OF IDS
6.6 COMPONENTS
6.7 TYPES
6.8 WHAT IS NOT AN IDS?
6.9 DETECTION METHODOLOGIES
6.10 VARIOUS TOOLS AVAILABLE
6.11 LIMITATIONS OF IDS
6.12 INTRUSION PREVENTION SYSTEM
6.13 TYPES
6.14 NETWORK BASED IPS
6.15 COUNTER MEASURES TAKEN BY AN IPS
6.16 RISKS INVOLVED

UNIT 7: HONEYPOTS

7.1 DESCRIBE HONEYPOTS
7.2 CATEGORIZED THE TYPES OF HONEYPOTS
7.3 DISCUSS THE ADVANTAGES AND DISADVANTAGES OF HONEYPOT
7.4 ILLUSTRATE HOW TO SETUP A HONEYPOT
7.5 DESCRIBE HONEYPOT: KFsensor, SPECTER, and HONEYD
7.6 LIST THE STEPS TO BE PERFORMED WHEN THE SYSTEM IS ATTACKED

UNIT 7: ACCESS CONTROL SYSTEM

7.7 INTRODUCTION: WHAT IS ACCESS CONTROL
7.8 ACCESS CONTROL IN PHYSICAL SECURITY
7.9 ACCESS CONTROL IN INFORMATION SECURITY
7.10 NEED OF AN ACCESS CONTROL SYSTEM
7.11 SOME CONCEPTS RELATED TO ACCESS CONTROL
7.12 POLICIES, MODELS, AND MECHANISMS
7.13 DISCRETIONARY ACCESS CONTROL (DAC)
7.8 NON-DISCRETIONARY ACCESS CONTROL
7.9 MANDATORY ACCESS CONTROL (MAC)
7.10 ROLE-BASED ACCESS CONTROL
7.11 TEMPORAL CONSTRAINTS
7.12 WORKFLOW
7.13 CHINESE WALL
7.14 ACCESS CONTROL MANAGEMENT INTRODUCTION

H.A LINKS SOLUTION

appin
The Information Security Specialist

MODULE: Hacking Attacks

UNIT 1: MALWARES

1.1 INTRODUCTION TO MALWARES
1.2 TYPES OF MALWARES
1.3 INSTALLING BOTS ON TARGET MACHINES
1.4 ATTACKING METHODS
1.5 WORKING OF BOTS
1.6 MALWARE DETECTION TECHNIQUES
1.7 COUNTER MEASURES

UNIT 2: VIRUS AND WORMS

2.1 INTRODUCTION TO VIRUSES
2.2 VIRUS AND WORMS STATISTICS 2012
2.3 WORKING OF VIRUSES: INFECTION PHASE
2.4 WORKING OF VIRUSES: ATTACK PHASE
2.5 WHY DO PEOPLE CREATE COMPUTER VIRUSES?
2.6 INDICATIONS OF VIRUS ATTACK
2.7 HOW DOES A COMPUTER GET INFECTED BY VIRUSES
2.8 TYPES OF VIRUSES
2.9 WRITING A SIMPLE VIRUS PROGRAM
2.10 COMPUTER WORMS
2.11 HOW IS A WORM DIFFERENT FROM A VIRUS?
2.12 EXAMPLE OF WORM INFECTION: CONFLICKER WORM
2.13 WHAT DOES WORM DO?
2.14 HOW DOES THE WORM WORK?
2.15 VIRUS DETECTION METHODS
2.16 VIRUS AND WORMS COUNTERMEASURES
2.17 ANTI-VIRUS TOOLS
2.18 PENETRATION TESTING FOR VIRUS

UNIT 3: TROJANS AND BACKDOORS

3.1 WHAT IS TROJAN?
3.2 PURPOSE OF TROJANS?
3.3 WHAT DO TROJAN CREATORS LOOK FOR?
3.4 INDICATIONS OF A TROJAN ATTACK
3.5 COMMON PORTS USED BY TROJANS
3.6 HOW TO INFECT SYSTEM USING A TROJAN?
3.7 DIFFERENT WAYS A TROJAN CAN GET INTO A SYSTEM
3.8 HOW TO DEPLOY A TROJAN>
3.9 EVADING ANTI-VIRUS TECHNIQUES
3.10 TROJAN COUNTERMEASURES
3.11 BACKDOOR COUNTERMEASURES
3.12 TROJAN HORSE CONSTRUCTION KIT
3.13 ANTI-TROJAN SOFTWARES

UNIT 4: HACKING ATTACKS

4.1 INTRODUCTION TO ATTACKS
4.2 TYPES OF ATTACKS
4.3 NON-TECHNICAL ATTACK
4.4 TECHNICAL ATTACKS
4.5 WHAT IS DENIAL OF SERVICE ATTACK
4.6 GAIN INSIGHTS ON DISTRIBUTED DENIAL OF SERVICE ATTACKS
4.7 EXAMINE THE WORKING OF DISTRIBUTED DENIAL OF SERVICE ATTACKS
4.8 ANALYZE SYMPTOMS OF A DoS AttacK
4.9 UNDERSTANDING INTERNET CHAT QUERY (ICQ)
4.10 UNDERSTANDING INTERNET RELAY CHAT (IRC)
4.11 ACCESS DoS AttacK TECHNNIQUES
4.12 ACCESS DoS/DDoS Attack Tools
4.13 DESCRIBE DETECTION TECHNIQUES
4.14 IDENTIFY DoS/DDoS Attack PROTECTION Tools
4.15 UNDERSTAND DoS/DDoS PENETRATION TESTING

UNIT 5: SESSION HIJACKING

5.1 UNDERSTAND WHAT IS SESSION HIJACKING
5.2 IDENTIFY Key Session Hijacking Techniques
5.3 UNDERSTAND BRUTE FORCING ATTACK
5.4 UNDERSTAND HTTP REFERRED ATTACK
5.5 SPOOFING vs. HIJACKING
5.6 UNDERSTAND SESSION HIJACKING PROCESS
5.7 IDENTIFY TYPES OF SESSION HIJACKING
5.8 UNDERSTAND APPLICATION LEVEL SESSION HIJACKING
5.9 DISCUSS SESSION SNIFFING
5.10 DESCRIBE Man-In-the-Middle Attack
5.11 UNDERSTAND Man-In-the-Middle Browser Attack
5.12 UNDERSTAND CLIENT SIDE ATTACK
5.13 UNDERSTAND Cross-Site-Scripting Attack
5.14 UNDERSTAND TCP/IP HIJACKING
5.15 IDENTIFY SESSION HIJACKING TOOLS
5.16 IDENTIFY COUNTERMEASURES OF SESSION HIJACKING
5.17 UNDERSTAND SESSION HIJACKING PEN TESTING

UNIT 6 : SQL INJECTION

6.1 UNDERSTAND SQL INJECTION
6.2 EXAMINE SQL INJECTION ATTACKS
6.3 UNDERSTAND WORKING OF WEB APPLICATIONS
6.4 IDENTIFY SERVER SIDE TECHNOLOGIES
6.5 UNDERSTAND SQL INJECTION DETECTION
6.6 TYPES OF SQL INJECTION
6.7 UNDERSTAN BLIND SQL INJECTION
6.8 LEARN SQL INJECTION METHODOLOGY
6.9 UNDERSTAND SQL QUERY
6.10 DESCRIBE PASSWORD GRABBING
6.11 IDENTIFY SQL INJECTION TOOLS
6.12 UNDERSTAND DEFENSIVE STRATEGIES AGAINST SQL INJECTION ATTACKS
6.13 IDENTIFY SQL INJECTION DETECTION TOOLS

UNIT 7: ART OF GOOGLING

7.1 INTRODUCTION
7.2 THE GOOGLE TOOLBAR
7.3 SEARCHING TECHNIQUES
7.4 DIRECTORY LISTING
7.5 LOCATING CGI-BIN
7.6 CAMERA HACKING
7.7 SOME TRICKS
7.8 MORE TRICKS

MODULE: Data Security

UNIT 1: INTRODUCTION

1.1 OVERVIEW
1.2 DATA SECURITY MANAGEMENT
1.3 CHARACTERISTICS OF ACCESS SECURITY IN THE SYSTEM
1.4 DATA SECURITY ISSUES AND SOLUTIONS

UNIT 2: DATA BACKUP

2.1 INTRODUCTION
2.2 DATA BACKUP STRATEGIES

UNIT 3: CRYPTOGRAPHY

3.1 CRYPTOGRAPHY
3.2 STRENGTH OF THE CRYPTOGRAPHY
3.3 GOALS OF CRYPTOGRAPHY
3.4 SOME TECHNICAL TERMS
3.5 TYPES OF CIPHER TEXT
3.6 TYPES OF CRYPTOGRAPHY
3.7 DATA ENCRYPTION STANDARD (DES)
3.8 IDEA: INTERNATIONAL DATA ENCRYPTION ALGORITHM
3.9 ASYMMETRIC CRYPTOGRAPHY
3.10 RSA ALGORITHM
3.11 HASH FUNCTIONS
3.12 DIGITAL SIGNATURES

UNIT 4: STAGENOGRAPHY

4.1 OVERVIEW
4.2 HOW DOES IT WORK?
4.3 STEGANOGRAPHY IN IMAGES
4.4 STEGANOGRAPHY IN AUDIO
4.5 GENETIC ALGORITHM APPROACH
4.6 STEGANOGRAPHY IN VIDEO

H.A LINKS SOLUTION

appin
The Information Security Specialist

MODULE: Cyber Forensics

UNIT 1: CYBER CRIME

1.1 INTRODUCTION TO CYBER FORENSICS
1.2 FORENSICS PROCEDURES
1.3 HISTORY OF COMPUTER FORENSICS
1.4 CYBER SECURITY & FORENSICS
1.5 WHAT IS CYBER CRIMES?
1.6 CYBER CRIMINALS
1.7 MODE AND MANNER OF COMMITTING CYBER CRIME
1.8 UNDERSTAND THE FUNDAMENTALS
1.9 CLASSIFICATION OF CYBER CRIME
1.10 WHY LEARN ABOUT CYBER CRIME
1.11 TYPES OF CYBER CRIME
1.12 CHARACTERISTICS OF COMPUTER CRIME
1.13 PREVENTION OF CYBER CRIME
1.14 QUESTIONNAIRE BASED ON RECOMMENDATIONS FROM THE FOURTH MEETING OF GOVERNMENTAL EXPERTS ON CYBER-CRIME

UNIT 2: CYBER FORENSICS

2.1 CYBER FORENSICS: DETAILED VIEW
2.2 DIGITAL EVIDENCE
2.3 CHALLENGES OF FORENSIC SCIENCE
2.4 FORENSIC METHODOLOGY
2.5 SOME FORENSIC SOFTWARES/ HARDWARES
2.6 BASIC APPROACHES
2.7 FORENSICS TOOLS EXAMPLE

UNIT 3: CATCHING CRIMINALS

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

MODULE: ISMS

UNIT 1: SECURITY AUDITING

1.1 INTRODUCTION
1.2 BACKGROUND
1.3 SECURITY AUDITING OBJECTIVES
1.4 RISK INVOLVED
1.5 AUDITING STEPS

UNIT 2: LEAD AUDITOR: IT (LA-27001)

2.1 INFORMATION SECURITY AND MANAGEMENT SYSTEM
2.2 MANAGING SECURITY AWARENESS
2.3 RISK ASSESSMENT, BUSINESS CONTINUITY AND DISASTER
2.4 SECURITY MANAGEMENT PRACTICES AND FRAMEWORK

MODULE: Cyber Laws and IT Acts

1.1 INTRODUCTION
1.2 CYBER LAWS: INTERNATIONAL PERSPECTIVE
1.3 E-GOVERNANCE
1.4 IMPEDIMENTS IN IMPLEMENTING E-GOVERNANCE PROJECTS FROM LEGAL PERSPECTIVE
1.5 ANALYSIS OF PROBLEMS - REPERCUSSIONS
1.6 RELEVANT LAWS
1.7 JURISPRUDENCE OF INDIAN CYBER LAW
1.8 THE INFORMATION TECHNOLOGY ACT, 2000 (SOME LAWS)
1.9 ADVANTAGES OF CYBER LAWS
1.10 PROSECUTION OF CYBER CRIMES UNDER INDIAN CYBER LAWS (IT ACT, 2000)
1.11 PROBABLE SOLUTIONS