Dear Sir/Madam,

I am delighted to inform you that IGNOU is ready to launch **PG Diploma in Information Security (PGDIS) (one year duration) (With an exit option of PG Certificate in Information Security (PGCIS) after successfully completion of first semester)** and **Advanced Certificate in Information Security (ACISE) (six month duration) (With an exit option of Certificate in Information Security (CISE) after successfully completion of first three courses of 12 Credits)**.

Please find enclosed the Programme Information Sheet and Performa of the Application to be completed and submitted to IGNOU.

Kindly note the following:

1) On receipt of your application by IGNOU and if found satisfactory, the process of inspection and approval of your Institute as Programme Study Centre (PSC) will be undertaken.

2) Institute will be communicated with regard to promotional efforts and admission process so as to commence the classes on schedule.

3) The filled in application along with supporting document may be sent to the address given below so that the same can reach us on or before 31-05- 2011.

   **Programme Co-ordinator**
   Room No. 19, Block-1
   SOVET, IGNOU
   Maidan Garhi
   New Delhi-110068

4) My Colleague, Ms. Urshla Kant, Assistant Professor, School of Vocational Education and Training, IGNOU is the Programme Coordinator for the above programmes. Please feel free to contact her either on her telephone No. 011-29571123 or her e-mail. urshlakant@ignou.ac.in for seeking any clarification.

5) In case you need any further clarification/ information please feel free to contact the school. We will be more than delighted to be of assistance to you.

We recognize your role and contribution to the success of this academic endeavour. The ultimate objective is being to fulfill the aspirations of our students and the need of the Information Security.

With kind regards,

Yours Sincerely,

(Prof. C.G. Naidu)
Director (SOVET)
INDIRA GANDHI NATIONAL OPEN UNIVERSITY
SCHOOL OF VOCATIONAL EDUCATION & TRAINING (SOVET)

Programme Information Sheet
(1) PG Diploma in Information Security (PGDIS)
(2) PG Certificate in Information Security (PGCIS) (With an exit option of PG Certificate in Information Security (PGCIS) after successfully completion of first semester)
(3) Advanced Certificate in Information Security (ACISE) (With an exit option of Certificate in Information Security (CISE) after successfully completion of first three courses of 12 Credits)

These innovative Programmes in the area of Information Security from IGNOU envisages to combine the strength of both IGNOU and Programme Study Centres to bridge the gap in awareness and competency required by various categories of people as the users of Internet and various IT enabled services about deeper aspects of Information Security, responsible use and management of IT services. Certification of skills would help them in getting gainful employment in the emerging global market. It incorporates the flexibility of open and distance learning with continuing education through the conventional system by way of Face-to-Face interaction at the Programme Study Centre (PSC) for both theory and practical components.

<table>
<thead>
<tr>
<th>Name of the Programme</th>
<th>(1) PG Diploma in Information Security (PGDIS)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(2) PG Certificate in Information Security (PGCIS)</td>
</tr>
<tr>
<td></td>
<td>(With an exit option of PG Certificate in Information Security (PGCIS) after successfully completion of first semester)</td>
</tr>
</tbody>
</table>

Programme Code
(1) PGDIS
(2) PGCIS
Number of Credits : 32
Duration : 1 Year
Medium of Instruction : English
Programme Fee : Rs. 8000/- (per semester)
Eligibility :
A. B.Sc (Computer Science)/ B.C.A/ B.Tech (Computer Sc.)/ B.Tech (IT) or its equivalent
B. Bachelor Degree in any discipline or its equivalent from the recognized University/ Institute with CIT/CIC from IGNOU
C. Bachelor Degree in any discipline or its equivalent from the recognized University/ Institute with 1 year working experience in Computer application/IT.
Course Details:

**Semester one:**

<table>
<thead>
<tr>
<th>Sl.No.</th>
<th>Course Code</th>
<th>Title of the course</th>
<th>Type of course compulsory/optional</th>
<th>Credits</th>
<th>Theory/Practical/Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>MSE-024</td>
<td>Policy, Standards and Laws</td>
<td>Compulsory</td>
<td>4</td>
<td>Theory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td></td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

**Semester Two:**

<table>
<thead>
<tr>
<th>Sl.No.</th>
<th>Course Code</th>
<th>Title of the course</th>
<th>Type of course compulsory/optional</th>
<th>Credits</th>
<th>Theory/Practical/Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>MSEI-026</td>
<td>BCP, DR Planning and Audit</td>
<td>Compulsory</td>
<td>4</td>
<td>Integrated (Theory &amp; Practical)</td>
</tr>
<tr>
<td>7.</td>
<td>MSEI-027</td>
<td>Digital Forensics</td>
<td>Compulsory</td>
<td>4</td>
<td>Integrated (Theory &amp; Practical)</td>
</tr>
<tr>
<td>8.</td>
<td>MSEP-028</td>
<td>Project</td>
<td>Compulsory</td>
<td>4</td>
<td>Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td></td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

**Structure of this Programme**

**PG Diploma in Information Security**

Duration : 1Year   Semester: 2 Semesters   No. of Credits: 32

(With an exit option of PG Certificate in Information Security after successfully completion of first semester)

**Target Group:**

A. B.Sc (Computer Science)/ B.C.A/ B.Tech (Computer Sc.)/ B.Tech (IT) or its equivalent

B. Bachelor Degree in any discipline or its equivalent from the recognized University/Institute with CIT/CIC from IGNOU

C. Bachelor Degree in any discipline or its equivalent from the recognized University/Institute with 1 year working experience in Computer application/IT.
1st Semester

Course 1: Introduction to Information Security– (4 Credits, Compulsory, Theory and Practical) : MSEI-021

Block 1: Business Needs and Security Awareness
Unit 1. Information Technology Concept and Application
Unit 2. Security Awareness
Unit 3. Information Security: Overview
Unit 4. Legal and Ethical Issues

Block 2: Security Threat and Vulnerability.
Unit 1. Introduction to Security threats and Vulnerability
   (Computer as a target, as a mean of resource or as a mean of attack)
Unit 2. Malware
   (Viruses, Worms, Trojan horses)
Unit 3. Hacking: Issues and Techniques
Unit 4. Security Counter Measures

Block 3: Networking Concepts and Attacks.
Unit 1. Introduction to Data Communication and Transmission Media
Unit 2. Overview of Networking technologies
   (Topologies)
Unit 3. Network Management and Protocol
Unit 4. Network Attacks

Block 4: Operating System Concepts
Unit 1. Introduction to Operating System
Unit 2. Operating System Security: An Overview
   (Authentication, Access controls, Security models, Updates, Patches, Integrity checks, Antivirus software)
Unit 3. Operating System Hardening and Controls
Unit 4. ADC/SAMBA
   (File servers)

Course 2: Network Security–(4 Credits, Compulsory, Theory and Practical): MSEI-022

Block 1: Introduction to Network Security
Unit 1. Network Security Concepts
   (Threats, Mechanism)
Unit 2. Network Security Techniques
   (Digital Water marking, ATC)
Unit 3. Identity Management
   (Biometrics, All Physical Security, login, Finger Printing)
Unit 4. Security Issues in Wireless and next generation networks
Block 2: Secure Protocols
Unit 1. Introduction to Secure Protocols
Unit 2. Specific Protocol-I
   (at network level eg. IPSec, VPN, SHCN, SSL)
Unit 3. Specific Protocol-II
   (at Application level eg. PGP, SHTTP, SSH etc)

Block 3: Cryptography Techniques
Unit 1. Introduction to Cryptography
Unit 2. Symmetric Key Cryptography
Unit 3. Asymmetric Key Cryptography
   (Hash function)
Unit 4. Applications of cryptography
   (Steganography, PK(Public key infrastructure), DH(Diffie-Hellman key), Electronic Signatures)

Block 4: Network Security Technology
   (Firewalls, Routers etc)
Unit 1. Firewalls
   (Network, Application and Host based Firewalls, Proxy)
Unit 2. IDS/IPS/Honey Pots
Unit 3. Scanning and Analysis Tools

Course 3: Cyber Security– (4 Credits, Compulsory, Theory and Practical): MSEI-023

Block 1: Information Gathering
Unit 1. Social Engineering
Unit 2. E-mail Crime and Investigation
Unit 3. Reverse Engineering
Unit 4. Cracking Methodology

Block 2: Database Security
Unit 1. Introduction to Database Concepts
Unit 2. Handon Database usage and Hacking Attempt
Unit 3. Database Security-I
   (Distributed Databases, Security aspects related to centralized Distributed Database)
Unit 4. Database Security-II
   (Concurrence, Failure recovery, Fault tolerance, Transaction theory)

Block 3: WEB Technology
Unit 1. Introduction to WEB Architecture
   (W3C)
Unit 2. Client Site Scripts
Unit 3. Server Site Scripts
Unit 4. Attacks on WEB Application

Block 4: Internet Technology
Unit 1. Internet Architecture
Unit 2. Social Networking Sites
Unit 3. Advanced Searching Techniques
   (Search engines like Google etc)
Unit 4. Latest trend in Internet Securities
   (Web 2.0)

Course 4: Policy, Standards and Laws—(4 Credits, Compulsory, Theory): MSE-024

Block 1: Security Standards
Unit 1. Introduction to Security Policies and Standards
   (Need, Methods, Various Standards: ISO 27001, HIPA, Vertical)
Unit 2. Security Framework Standards
   (ISO Standards-all)
Unit 3. Security Mechanism Standards
   (Encryption, Digital Signatures, Techniques, Algorithm)
Unit 4. Security Protocol Standards
   (Entity authentication protocol, Key establishment, Time stamping)

Block 2: ISO Standards
Unit 1. Study of ISO Standards: A complete Case Study

Block 3: Cyber Laws
Unit 1. International Treaties, Conventions and Protocols concerning cyberspace
   (Guidelines issued by various ministries, Alternative Dispute Resolution, Online Dispute Resolution)
Unit 2. Information Technology Amendment Act 2008-I
   (In Introduction: Criminal Law & Constitutional Law in brief)
Unit 3. Information Technology Amendment Act 2008-II
   (Limitations)
Unit 4. Cyberspace and IPR
   (Search engines, Web crawling, Indexing, searching, Ranking of web pages, Spamdexing)

Block 4: Cyber Crimes and Regulation
Unit 1. Introduction to Computer Crimes
Unit 2. Conventional Crimes through Computer
Unit 3. Crimes and Torts committed on a Computer Network
Unit 4. Crimes relating to Data Alteration/ Destruction/ Theft of source code and Database
   (Online Dispute Resolution, theft of source code; a case study)

2nd Semester

Course 5: Application and Business Security Developments— (4 Credits, Compulsory, Theory and Practical): MSEI-025

Block 1: Application Development Life Cycle
Unit 1. Application Design
Unit 2. Application Coding
Unit 3. Application Testing
Unit 4. Application Production and Maintenance

Block 2: Secure Application Development-I
Unit 1. Critical Application Security Concepts
Unit 2. Input Validation and Encoding
Unit 3. Authentication, Authorization and Session Management
Unit 4. Encryption, Confidentiality and Data Protection

Block 3: Secure Application Development -II
Unit 1. Data Access
Unit 2. Error Handling and Logging
Unit 3. Server Configuration and Code Management
Unit 4. Application Threat Modeling

Block 4: Application Testing and Ethical Hacking
Unit 1. Assessment Methodologies and Tools
Unit 2. Application Security Assessments
Unit 3. WEB Application Scanning and Vulnerability Assessment
Unit 4. WEB Application Ethical Hacking

Course 6: BCP, DR Planning and Audit– (4 Credits, Compulsory, Theory and Practical) : MSEI-026

Block 1: Risk Analysis
Unit 1. Introduction to Risk Analysis
Unit 2. Risk Assessment
Unit 3. Risk Analysis Techniques and Methodologies
Unit 4. Risk Mitigation

Block 2: Business Continuity
Unit 1. Need for a Business Continuity Program
Unit 2. Overview of Business Continuity Management Life Cycle
Unit 3. Defining Organization’s Business Continuity Requirements
Unit 4. Identifying and Selecting Business Continuity Strategies

Block 3: DR Strategies
Unit 1. Developing Plans for Computer System Recovery
Unit 2. Developing Plans for Business Resumption
Unit 3. Plan Templates and Software Tools
Unit 4. Implementing Crisis Management Framework

Block 4: BCM Program Management
Unit 1. Maintaining and Administering BCM Plans
Unit 2. Auditing and Evaluating BCM plans
Unit 3. Developing and Implementing a BCM Response
Unit 4. Disaster Simulation Exercise
Course 7: Digital Forensics – (4 Credits, Compulsory, Theory and Practical) : MSEI-027

Block 1: Cyber Crime and Cyber Forensics
Unit 1. Various Types of Cyber Crimes
Unit 2. Banking and Financial Crimes
Unit 3. Identify Thefts and Data Thefts/ Source Code Thefts
Unit 4. SPAM and BOTNETS
   (1 Case Study on Nigerian Letter Fraud)

Block 2: Digital Forensics
Unit 1. Digital Investigation
Unit 2. Data Acquisition and Information Gathering
Unit 3. Forensic Examination of Systems
   (Keyword, Data recovery, Various tools NKS)
Unit 4. Forensic Examination of Network Devices
   (Routers, Firewalls, IDS/IPS etc)

Block 3: Mobile Forensics
Unit 1. Introduction to Mobile Forensics and Technologies
Unit 2. Analysis of CDR’s
Unit 3. Application of SIM Card Reader’s
Unit 4. Forensic Examination of Mobile Devices
   (Mobile Frauds)

Block 4: Security Issues in Wireless Technologies
Unit 1. Introduction to Wireless Technologies
Unit 2. Wireless Devices
Unit 3. Securing Wireless Network
Unit 4. Ethical Hacking- Wireless Security

Course 8: MSEP-028 Project– 4 Credits
Name of the Programme: (3) Advanced Certificate in Information Security (ACISE) (With an exit option of Certificate in Information Security (CISE) after successfully completion of first three courses of 12 Credits)

Programme Code: ACISE

Number of Credits: 18

Duration: 6 Months

Medium of Instruction: English

Programme Fee: Rs. 4000/- (one time)

Eligibility: 10th or its equivalent

Course Details:

<table>
<thead>
<tr>
<th>Sl.No.</th>
<th>Course Code</th>
<th>Title of the course</th>
<th>Type of course compulsory/optional</th>
<th>Credits</th>
<th>Theory/Practical</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>OSEI-041</td>
<td>Information Security</td>
<td>Compulsory</td>
<td>4</td>
<td>Integrated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Theory &amp; Practical)</td>
</tr>
<tr>
<td>2.</td>
<td>OSEI-042</td>
<td>Securing Internet Access</td>
<td>Compulsory</td>
<td>4</td>
<td>Integrated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Theory &amp; Practical)</td>
</tr>
<tr>
<td>3.</td>
<td>OSE-043</td>
<td>Information Technology Security</td>
<td>Compulsory</td>
<td>4</td>
<td>Theory</td>
</tr>
<tr>
<td>4.</td>
<td>OSEI-044</td>
<td>Server Security</td>
<td>Compulsory</td>
<td>6</td>
<td>Integrated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Theory &amp; Practical)</td>
</tr>
</tbody>
</table>

Total 18

Structure of this Programme

Advanced Certificate in Information Security

Duration: 6 Months  No. of Credits: 18

(With an exit option of Certificate in Information Security after successfully completion of first three courses of 12 Credits)

Target Group: 10th Pass or its equivalent

Course 1: Information Security– (4 Credits (1 Credit-Theory and 3 Credit-Practical), Compulsory) : OSEI-041

Block 1: Overview of Information Security
Unit 1. Information Security Concepts
(How to Secure Software)

Unit 2. User Habits
Unit 3. Threats, Vulnerability and Malware
(Viruses, Worms, Trojan horses)

Unit 4. Impact of Hardware and Software Protocols with Preventive Measures

Block 2: Securing Desktop
Unit 1. Securing Desktop Concerns
Unit 2. Securing Files and Folders with Password
(Poweron Password, Login Password)
Unit 3. User Restricted Data, Sharing of Files and Secure Downloading from Internet
Unit 4. Security Threats due to Software Piracy

Block 3: Securing Data
Unit 1. Securing, Backup and Restore Strategies for Data
Unit 2. Concepts of PC auditing
Unit 3. Snapshot Utility
Unit 4. Defragmentation

Block 4: Securing Connectivity
Unit 1. Secure Network Connectivity
Unit 2. Firewalls
Unit 3. Encryption
Unit 4. Using some secure protocols

Course 2: Securing Internet Access—(4 Credits (1 Credit-Theory and 3 Credit-Practical), Compulsory) : OSEI-042

Block 1: Secure Browsing
Unit 1. Browsing History
Unit 2. Cookies, E-mail and Internet Applications
Unit 3. Log Files, Plug-ins and Scripts
Unit 4. Protecting from Fake Websites

Block 2: Internet Transaction Security
Unit 1. Secure Protocols
Unit 2. Privacy policies
Unit 3. How Identity Theft Works and its Prevention
Unit 4. Credit Card Fraud

Block 3: Securing Web Services
Unit 1. Security Challenges Specific to Web Services
Unit 2. Web Application Security Testing
Unit 3. Cyber Forensics, Digital Certificates and Digital Watermarking
Unit 4. Threat Profile, Risk Analysis and Defence Against Threats

Block 4: Securing during Mobility
Unit 1. Security in Wireless Environment
Unit 2. Wi-fi, Blue tooth, LAN
Unit 3. Digital Incident Response
Unit 4. Industry Perspective
Course 3: Information Technology Security— (4 Credits-Theory, Compulsory) : OSE-043

Block 1: W3C Compliance
Unit 1. Introduction to W3C
Unit 2. Recommendations and certifications of W3C
Unit 3. W3C Standards and Practices
Unit 4. How do we Improve Internet Privacy using W3C

Block 2: Introduction to ISO 27000
Unit 1. Need of Certification
Unit 2. ISO/IEC 27000 family of Information Security Management Systems (ISMS) standards
Unit 3. Cyber Security Standards
Unit 4. Employee perspective of ISO 27000

Block 3: Information Technology Act
Unit 1. Introduction to Information Technology Amendment Act 2008
    (Unique ID (UID), Limitations of Information Technology Amendment Act 2008)
Unit 2. Legal Implications of Personal Security
Unit 3. Common Cyber Crimes and Government Laws and Rules in Information security

Course 4:– Server Security (6 Credits (1 Credit-Theory and 5 Credit-Practical), Compulsory): OSEI-044

Block 1: Email Security
Unit 1. Email Servers
Unit 2. Email Forgery and Spamming
Unit 3. Password Attack Vectors
Unit 4. Account Security

Block 2: Windows Security
Unit 1. Windows System Architecture
Unit 2. Windows System Security
Unit 3. Hacking Windows

Block 3: Linux Security
Unit 1. Linux System Architecture
Unit 2. Linux System Security
Unit 3. Hacking Linux

Block 4: Webserver Security
Unit 1. Understanding Web Technologies
Unit 2. Web Application Attacks

Block 5: Wireless Network Security
Unit 1. Wireless Network Concepts
Unit 2. Wireless Attacks
Unit 3. Wireless Security Measures
Block 6: Software Security
Unit 1. Recovering Software Codes
Unit 2. Understanding Software Code
Unit 3. Developing Software Patches and Code

Note: All applicable topics should be explained for Open office and MS-Word.

The eligibility conditions for the academic counselors for both theory and practical are as follows:

A) For PG Diploma in Information Security (PGDIS) (one year duration) (With an exit option of PG Certificate in Information Security (PGCIS) after successfully completion of first semester)
   Qualification: MCA/ M.Tech/ B.Tech/ B.E (CSE/IT) with relevant experience of 2 years

B) Advanced Certificate in Information Security (six month duration) (With an exit option of Certificate in Information Security after successfully completion of first three courses of 12 Credits)
   Qualification: Graduate and adequate familiarity to Internet and basic computer system
INDIRA GANDHI NATIONAL OPEN UNIVERSITY
SCHOOL OF VOCATIONAL EDUCATION & TRAINING

Application, Norms and Standards to become an Approved Programme Study Centre (PSC) for **PG Diploma in Information Security (PGDIS) (one year duration) (With an exit option of PG Certificate in Information Security (PGCIS) after successfully completion of first semester)** and **Advanced Certificate in Information Security (ACISE) (six month duration) (With an exit option of Certificate in Information Security (CISE) after successfully completion of first three courses of 12 Credits)**

Guidelines for applying:

1. The Institute must be a Registered Society/Trust/Company.

2. Softwares and equipment required for the Computer Laboratory which are window based licensed and open source

   **B) For PG Diploma in Information Security (PGDIS) (one year duration) (With an exit option of PG Certificate in Information Security (PGCIS) after successfully completion of first semester)**

   **Course 1: Introduction to Information Security – (4 Credits, Compulsory, Theory and Practical)**

   **Block 1: Business Needs and Security Awareness**

   **Block 2: Security Threat and Vulnerability.**

   Unit 1. Introduction to Security threats and Vulnerability
   BFB Tester
   CROSS (Codenomic Robust Open Source Software
   Gendrame
   Metasploit
   Nessus (Sedulity OS EH Edition)
   Niko
   Wireshark (Sedulity OS EH Edition)
   Oedipus
   Paros
   Flaw Finder

   **Unit 2. Malware**
   Nuclear RAT V2.XX
   SubSeven
   Turkojan4.exe
   Hydra
   etherflood.zip
   iris.zip
   networkview.exe
   smac20_setup.exe
   snort-2.8.6.1.tar.gz
   Snort_2_8_6_1_Installer.exe
   NetBus
   Back Orifice
   wireshark-win32-1.4.0.exe
Unit 3. Hacking: Issues and Techniques
NovaBACKUP
DT Utilities
PC Backup
Genie Backup Manager
Acronis True Image
NTI Backup Now
Acronis Backup & Recovery Norton Ghost
PowerBackup
BullGuard Backup
TurboBackup
Nmap
snort
netcat
Metasploit
Kismet
Nikto
Ethercap
GFI LanGaurd
Super Scan
Retina

Unit 4. Security Counter Measures
firestarter-1.0.3.tar.gz
kerio-kwf-whql-6.7.1-6399-win32.exe
kmyfirewall-1.1.1.tar.bz2
NPF_Retail(2).EXE
zapSetup_93_037_000_en.exe
snort
Windows/ Linux Firewall
Zone Alarm Pro
Segate Personal Firewall

Block 3: Networking Concepts and Attacks.
Unit 1. Introduction to Data Communication and Transmission Media
subnet calculator
Angry IP Scanner

Unit 2. Overview of Networking technologies
RouterWatchDemoSetup.exe
SolarWinds-Subnet-Calculator.exe
bos_sub.exe
TCPtraceroute
Tctrace
itrace

Unit 3. Network Management and Protocol
Wireshark (Sedulity OS EH Edition)
cain and abel
Ethercap

Unit 4. Network Attacks
doshttp_setup.exe
c_a_setup.exe
dsniff-2.3(2).tar.gz
dsniff-2.3.tar.gz
etherflood.zip
iris.zip
networkview.exe
smac20_setup.exe
snort-2.8.6.1.tar.gz
Snort_2_8_6_1_Installer.exe
wireshark-win32-1.4.0.exe
Sniffers
1. DSniff
2. Ettercap
3. Ettercap-GTK
4. ntop
5. SMBRelay3
6. SSLDump
7. Tcpick
8. Wireshark
9. xspy

Block 4: Operating System Concepts
Unit 1. Introduction to Operating System
Unit 2. Operating System Security: An Overview
john-16w
kerbcrack
lc4setup.exe
lc5setup.exe
legion
lns.exe
makestrm.exe
md5sum.exe
Merge Streams
nbname.cpp
nbtdeputy
NTFS and ADS.htm
ntinfoscan.exe
NTLM Authentication.ppt
Nt_rootkit0.40
Offline NT Password Resetter
psexec
pwdump2
pwdump3v2
remexec
1. 5nmap
2. Autoscan
3. Nmap
4. onesixtyone
5. p0f
6. Protos
7. sslscan
8. Xprobe2
9. Zenmap

Unit 3. Operating System Hardening and Controls
opt crack
lopth crack
gpedit

Unit 4. ADC/SAMBA
Windows ADC installation and setups
Course 2: Network Security–(4 Credits, Compulsory, Theory and Practical)

Block 1: Introduction to Network Security

Unit 1. Network Security Concepts
ips scanner
port scanners
Nmap
netcat
whois

Unit 2. Network Security Techniques
port blockers
IDS and Firewall
Network monitoring and Tracking
logs maintains

Unit 3. Identity Management
LaptopAlarmSetup.exe
nTracker_Trial.zip
TrueCrypt Setup 7.0a.exe
truencrypt-7.0a-linux-x86.tar.gz
websetupLite.exe

Unit 4. Security Issues in Wireless and next generation networks
Backtrack4.0
Airsnarf - A rogue AP setup utility.htm
Airsnort
Cqure AP
NetStumblerInstaller.exe
WEPCrack
WiFiScanner-Linux
Wireless Hacking Tools
Wireless Security Tools.htm
airopeek.exe
airsnarf-0.2.tar.gz
arpnoison
kismet
widzv1
wlanexpert
*.Aircrack -ng
*.Airmong-ng
*.Airodump-ng
*.AirSnarf
*.ASLEAP
*.Cowpatty
*.Genpmk
*.Kismet
*.Mackchanger
*.WEPbuster
2.Cracking
*.Aircrack -ng
*.Airmong-ng
*.Airodump-ng
*.AirSnarf
*.ASLEAP
*.Cowpatty
Bluetooth
1. Blueprint
2. BlueSmash
3. Btcsanner
4. Minicom
5. obexFtp
6. Ussp-Push

RFID
1. RFIDIOt Frosch
2. RFIDIOt Frosh
3. RFIDIOt PCSC

Block 2: Secure Protocols
Implementation of https
Implementation of smtps
Implementation of Ssh

Block 3: Cryptography Techniques
Unit 1. Introduction to Cryptography
Unit 2. Symmetric Key Cryptography
Unit 3. Asymmetric Key Cryptography
Unit 4. Applications of cryptography

Microsoft Cryptography tools
cert2spc.exe
MakeCat.exe
signer.dll.zip
stool.exe
wondercrypt
encryptor

Block 4: Network Security Technology
Unit 1. Firewalls
firestarter-1.0.3.tar.gz
kerio-kwf-whql-6.7.1-6399-win32.exe
kmyfirewall-1.1.1.tar.bz2
NPF_Retail(2).EXE
zapSetup_93_037_000_en.exe
snort
Firewall
ADMmutate-0.8.1.tar.gz
bro-1.5-release.tar.gz
nidsbench.tar.gz
Blackice

Unit 3. Scanning and Analysis Tools
tripwire-2.3.1-2.tar.gz
tcpreplay-3.4.4.tar.gz
fragroute-1.2.tar.gz
AntiFirewall
backstealth
dnsdigger.zip
firewalk

Portscanning
1. Autoscan
2. Nmap
3. propecia
4. UnicornScan
5. Zenmap

Service Fingerprinting
1. Amap
2. Htprint
3. Htprint_GUI

Identify Live Hosts
1. 0trace
2. 5nmp
3. Autoscan
4. Fping
5. Hping2
6. Hping3
7. Netdiscover
8. Nmap
9. onesixtyone
10. sslscan
11. TCPtraceroute
12. Zenmap

Network Mappings
1. 5nmp
2. Amap
3. Htprint
4. Htprint_GUI
5. Autoscan

6. Fping
7. Hping2
8. Hping3
9. P0f
10. ike-scan
11. Netdiscover
12. Netmask

13. Nmap
14. onesixtyone
15. Propecia
16. PSK-Crack
17. sslscan
18. XProbe2
19. 0trace
20. TCPtraceroute
21. Protos
22. UnicornScan
23. Zenmap

Identify Live Hosts
1. 0trace
2. 5nmp
3. Autoscan
Course 3: Cyber Security—(4 Credits, Compulsory, Theory and Practical)

Block 1: Information Gathering

Unit 1. Social Engineering

Unit 2. E-mail Crime and Investigation
65Advanced Stealth Email Redirector.zip
aep.zip
Email_Spider_Easy.zip
empasrec.zip
freesmtp.zip
mailpv.zip
MSN Explorer Password Recovery Software.exe
Nucleus-MSN-Password.exe
SECRET_INSTALL.EXE
smtpserver.exe
Yahoo Messenger Archive Recovery Software.exe
Exim/ Postfix MTA configuration

Unit 3. Reverse Engineering
3568_ResHack.zip
adc-0.69.zip
boomerang-linux-alpha-0.3.tar.gz
boomerang-win32-alpha-0.3.1.zip
hw32v601.exe
idademo54.exe
PE.Explorer_setup.exe
PE.Explorer_setup.zip
spices.zip
spicesdc.zip
Hex Edit
Evans Debugger
OllyDBG

Unit 4. Cracking Methodology
65Advanced Stealth Email Redirector.zip
FlexiSpy.rar
remotedesktopspy-setup.exe
spybuddy-setup-sw.exe
spyhunterS.exe
WCASSU54.exe
007PWD11.EXE
Accent_Office_Password_Recovery_1[1].02_by_AmoK
CMOSDEL.EXE
John the ripper
M0ong4B0oNg4.zip
NeverExpire.msi
advanced i messanger password recovery
aopb.zip
aoxppr_p.zip
ares.zip
ariskkey.exe
brutus-aet2.zip
brutusaet2.zip
setup_akll.exe
Perfect Keylogger.exe
XP Logon Password Logger.exe
Log Monitors.zip
iks2k20d.exe
E-Mail Keylogger.exe

VPN
1.iike-scan
2.PSK-Crack

SMB Analysis
1.SMBCClient.py

Password Attacks
1.Password offline Attacks
   *.bkhive
   *.john
   *.samdump2
   *.sqlpat
   *.wyd
2.password online attacks
   *.BruteSSH
   *.hydra
   *.Lodowep
   *.Medusa
   *.SSHater
   3.chntpw

Block 2: Database Security
Unit 1. Introduction to Database Concepts
MySQL Server Configuration

Unit 2. Hand on Database usage and Hacking Attempt
Blindfolded_SQL_Injection.pdf
DataThief
MSSQL Server Named Pipe Privilege Escalation Exploit.htm
Manipulating Microsoft SQL Server Using SQL Injection.doc
Microsoft SQL Server DoS Remote Exploit (MS03-031).htm
Oracle Auditing Tools
Oracle SID Enumeration
Oracle SQL Injection.mht
Oracle XDB FTP Service UNLOCK Buffer Overflow Exploit.htm
PHP-NUKE version = 6.9 cid sql injection Remote Exploit.htm
Unit 3. Database Security-I
Security and Privledges for MySQL Database

Unit 4. Database Security-II
Implementation of Security Policies

Block 3: WEB Technology

Unit 1. Introduction to WEB Architecture

Unit 2. Client Site Scripts
Java Script on Web Server like Apache

Unit 3. Server Site Scripts
PHP Server Side Script Implementation

Unit 4. Attacks on WEB Application
32 Bit IP Resolver
Automatic-Printing-in-IE Vulnerability.htm
Brute Force Attack Estimator.xls
Form Bookmarklets.url
Form Bookmarks.htm
Generate Unicode Strings.htm
Generate Xss Exploit
HTTP File Stealing
HelpMe2.pl
IE Cache Extractor
IEEN
IISHACK.doc
Running this page will crash IE.htm
WinDNSSpoof
hacking web servers
http traffic monitor
ieflaw
iehist-win32-0_0_1.zip
jad
lynx
monkeyshell.tar.gz
readme.htm
sitedigger
  1.ASP-Audit
  2.Burpsuite
  3.CSRPTester
  4.Curl
  5.DirBuster
  4.Grabber
  5.Grendel scan
  6.Httprint
  7.Httprint_GUI
  8.Lbd
  9.List-Urls
  10.Mini_Mysqlator
  11.Nikto
  12.Paros Proxy
  13.Ratproxy
  14.Swfintruder
  15.W3AF
  16.Wapti
  17.Webshag
  18.Wfuzz
Nessus Server
Nessus

**Block 4: Internet Technology**

**Unit 1. Internet Architecture**

**Unit 2. Social Networking Sites**
Browsers like firefox, Opera, Crome

**Unit 3. Advanced Searching Techniques**
googal hacking methodologies

**Unit 4. Latest trend in Internet Securities**
Virtualization of Servers

**Course 4: Policy, Standards and Laws–(4 Credits, Compulsory, Theory)**

**Block 1: Security Standards**

**Block 2: ISO Standards**

**Block 3: Cyber Laws**

**Block 4: Cyber Crimes and Regulation**

**2nd Semester**

**Course 5: Application and Business Security Developments– (4 Credits,**

**Block 1: Application Development Life Cycle**
Block 2: Secure Application Development-I

Block 3: Secure Application Development -II

Block 4: Application Testing and Ethical Hacking
ManageEngine_ApplicationsManager.exe
Nessus-3[1].2.1.1.exe
nsauditor_setup.exe

\textit{Portscanners}
PFSETUP1.EXE
PORTSCAN.EXE
SITESCAN.ZIP
nmap-3.55-SP2-win32.zip
nmapwin_1.3.1.exe
sup3rsc4n.zip
ws_ping_pro.zip

\textbf{Portscanning}
1. Autoscan
2. Nmap
3. propecia
4. UnicornScan
5. Zenmap

\textbf{Service Fingerprinting}
1. Ammap
2. Httprint
3. Httprint_GUI

\textbf{Course 6: BCP, DR Planning and Audit}– (4 Credits, Compulsory, Theory and Practical)

Block 1: Risk Analysis

Block 2: Business Continuity

Block 3: DR Strategies

Block 4: BCM Program Management

\textbf{Course 7: Digital Forensics}– (4 Credits, Compulsory, Theory and Practical)

Block 1: Cyber Crime and Cyber Forensics

Block 2: Digital Forensics
Unit 1. Digital Investigation

Unit 2. Data Acquisition and Information Gathering

Unit 3. Forensic Examination of Systems
FTK-Forensic_Toolkit-1.81.5.exe
EnCase Setup.exe
steller Data acquisition.exe
QuickRecoveryDemoLINUX.exe

Unit 4. Forensic Examination of Network Devices

\textbf{Block 3: Mobile Forensics}
Unit 1. Introduction to Mobile Forensics and Technologies
Unit 2. Analysis of CDR’s

Unit 3. Application of SIM Card Reader’s

Unit 4. Forensic Examination of Mobile Devices
AD_Mobile phone examiner.zip
MobileInspector.exe
OPM_Forensic_Trial_Setup.exe
memory-card-data-recovery-demo.exe
open folder.pps
sim-card.exe

Block 4: Security Issues in Wireless Technologies
Unit 1. Introduction to Wireless Technologies

Unit 2. Wireless Devices

Unit 3. Securing Wireless Network
Wireless Security Tools.htm
Elcomsoft Wireless Security Auditor 3.2.0.395
LucidLink Home Office Edition 2.2
PW0-200 - Wireless Security Professional (WSP) Practice Test Questions 1.0
AirStop Wireless 2.4.3

Unit 4. Ethical Hacking- Wireless Security
Airsnarf - A rogue AP setup utility.htm
Airsnort
Cqre AP
NetStumblerInstaller.exe
WEPCrack
WiFiScanner-Linux
Wireless Hacking Tools
airopeek.exe
airsnarf-0.2.tar.gz
arppoiison
kismet
widzv1
wlanexpert

Wireless Network Anaysis (Linux)
Bluetooth
1.Blueprint
2.BlueSmash
3.Btcsanner
4.HCIDump
5.Minicom
6.obexFtp
7.Ussp-Push

RFDI
1.RFIDIOt Frosch
*.Brute Force Hitag2
*.Bruteforce Mifare
*.Calculate JCOP MIFARE Keys
*.Continues Delect Tag
*.Copy ISO15693 TAG
*.ePassport READ WRIE CLONE
*.Format MIFARE 1k Value Blocks
1. All
   * Aircrack -ng
   * Airmon-ng
   * Airodump-ng
   * AirSnarf
   * ASLEAP
   * Cowpatty
   * Genpmk
   * Kismet
   * Mackchanger
   * WEPbuster

2. Cracking
   * Aircrack -ng
   * Airmon-ng
   * Airodump-ng
   * AirSnarf
   * ASLEAP
   * Cowpatty
   * Genpmk
   * Kismet
   * WEPbuster
B) Advanced Certificate in Information Security (ACISE) (six month duration)
(With an exit option of Certificate in Information Security (CISE) after successfully completion of first three courses of 12 Credits)

Course 1: Information Security– (4 Credits (1 Credit-Theory and 3 Credit-Practical), Compulsory)

Block 1: Overview of Information Security
Unit 1. Information Security Concepts (Testing Tools)
BFB Tester
CROSS (Codenomicon Robust Open Source Software
Gendrame
Metasploit
Nessus (Sedulity OS EH Edition)
Niko
Wireshark (Sedulity OS EH Edition)
Oedipus
Paros
Flaw Finder

Unit 2. User Habits
Encryptor
Windows/Linux Firewall
Security Settings as per Operating System
WonderCrypt
FileCrypto
Anti Virus
Setup of Wiif’s

Unit 3. Threats, Vulnerability and Malware
Nuclear RAT V2.XX
SubSeven
Turkojan4.exe
etherflood.zip
iris.zip
networkview.exe
smac20_setup.exe
snort-2.8.6.1.tar.gz
Snort_2_8_6_1_Installer.exe
NetBus
Back Orifice
wireshark-win32-1.4.0.exe
Hydra (Sedulity OS EH Edition)

Unit 4. Impact of Hardware and Software Protocols with Preventive Measures
Metasploit
Nessus (Sedulity OS EH Edition)
Niko
Wireshark (Sedulity OS EH Edition)
Oedipus

Block 2: Securing Desktop
Unit 1. Securing Desktop Concerns Theory

Unit 2. Securing Files and Folders with Password
AxCrypt
WinCry
Folder Guard

Unit 3. User Restricted Data, Sharing of Files and Secure Downloading from Internet
SFTP
Kodak EasyShare
Internet Download Manager softwares

Unit 4. Security Threats due to Software Piracy

Block 3: Securing Data
Unit 1. Securing, Backup and Restore Strategies for Data

Unit 2. Concepts of PC auditing
SystemMechanic7Pro.exe
WinAudit.exe
Nessus (Sedulity OS EH Edition)
Ratina

Unit 3. Snapshot Utility
systracer_setup_en.exe
Virtualization

Unit 4. Defragmentation
Auslogics Disk Defrag
Smart Defrag 1.5
JK Defrag
PageDefrag
SpeeDefrag
Diskeeper
OS Based Defragmentation

Block 4: Securing Connectivity
Unit 1. Secure Network Connectivity
NovaBACKUP
DT Utilities
PC Backup
Genie Backup Manager
Acronis True Image
NTI Backup Now
Acronis Backup & Recovery Norton Ghost
PowerBackup
BullGuard Backup
TurboBackup
Nmap
snort
netcat
Metasploit
Kismet
Nikto
Ethercap
GFI LanGaurd
Super Scan
Retina

Unit 2. Firewalls
firestarter-1.0.3.tar.gz
Unit 3. Encryption
afe_setup.exe
ahtmllepp109_setup.exe
encryptmyfolder.exe
glue.zip
StegSpy2.1.zip
stool.exe
Microsoft Cryptography tools
cert2spc.exe
MakeCat.exe
signer.dll.zip
Stools
Encryptor
WonderCrypt

Unit 4. Using some secure protocols
Implementation of https
Implementation of smtps
Implementation of Ssh

Course 2: Securing Internet Access—(4 Credits (1 Credit-Theory and 3 Credit-Practical), Compulsory)

Block 1: Secure Browsing
Unit 1. Browsing History
Pop-up History 0.0.3
Private Browsing 1.2.9
Attention Recorder 0.65
WinSettings 8.1
Trackless 1.03
Squid
logs
firefox, chrome, mozilla

Unit 2. Cookies, E-mail and Internet Applications
65Advanced Stealth Email Redirector.zip
aep.zip
Email_Spider_Easy.zip
empasrec.zip
freesmtpl.zip
mailpv.zip
MSN Explorer Password Recovery Software.exe
Nucleus-MSN-Password.exe
SECRET_INSTALL.EXE
smtpserver.exe
Yahoo Messenger Archive Recovery Software.exe
Portable Historian 1.4.4.0
pidgin
TeamViewer
Unit 3. Log Files, Plug-ins and Scripts
Active LogView 2.09.1.7378
XFile 2.021
ksLogger 1.17
logs

Unit 4. Protecting from Fake Websites
Netcraft Toolbar
GeoTrust TrustWatch
TrustToolbar
Clear Search Anti-Phishing
BullGuard Internet Security (32-bit version)
phishing protection from the browsers
Thunderbird Security

Block 2: Internet Transaction Security

Unit 1. Secure Protocols
https implementation
smtps implementations
ssh (secure shell)

Unit 2. Privacy policies
IP tables
Firewalls
User authentications

Unit 3. How Identity Theft Works and its Prevention
MySecurityVault PRO
MyIdentityDefender Toolbar
Identity Theft Protector
TrustedID Identity Theft Protection
Identity Theft Toolkit

Unit 4. Credit Card Fraud

Block 3: Securing Web Services
Unit 1. Security Challenges Specific to Web Services
webInjext

Unit 2. Web Application Security Testing
32 Bit IP Resolver
Automatic-Printing-in-IE Vulnerability.htm
Brute Force Attack Estimator.xls
Form Bookmarklets.url
Form Bookmarks.htm
Generate Unicode Strings.htm
Generate Xss Exploit
HTTP File Stealing
HelpMe2.pl
IE Cache Extractor
IEEN
IISHACK.doc
Running this page will crash IE.htm
WinDNSSpoof
hacking web servers
http traffic monitor
ieflaw
iehist-win32-0_0_1.zip
jad
lynx
monkeyshell.tar.gz
readme.htm
sitedigger
Odysseus
metaexploit
Paros Proxy

Unit 3. Cyber Forensics, Digital Certificates and Digital Watermarking
FTK-Forensic_Toolkit-1.81.5.exe
EnCase Setup.exe
steller Data acquisition.exe
QuickRecoveryDemoLINUX.exe

Web Analysis
1. ASP-Audit (Sedulity OS EH Edition)
2. Burpsuite (Sedulity OS EH Edition)
3. CSRPTester (Sedulity OS EH Edition)
4. Curl (Sedulity OS EH Edition)
5. DirBuster (Sedulity OS EH Edition)
4. Grabber
5. Grendel scan (Sedulity OS EH Edition)
6. Httpprint (Sedulity OS EH Edition)
7. Httpprint_GUI (Sedulity OS EH Edition)
8. Lbd (Sedulity OS EH Edition)
9. List-Urls (Sedulity OS EH Edition)
10. Mini Mysqlator (Sedulity OS EH Edition)
11. Nikto (Sedulity OS EH Edition)
12. Paros Proxy (Sedulity OS EH Edition)
13. Ratproxy (Sedulity OS EH Edition)
14. SwfIntruder (Sedulity OS EH Edition)
15. W3AF (Sedulity OS EH Edition)
16. Wapti (Sedulity OS EH Edition)
17. Webshag (Sedulity OS EH Edition)
18. Wfuzz
19. ZZuff (Sedulity OS EH Edition)
20. Webscarb Lite (Sedulity OS EH Edition)
Nessus Server (Sedulity OS EH Edition)
Nessus (Sedulity OS EH Edition)

Unit 4. Threat Profile, Risk Analysis and Defence Against Threats
ManageEngine_ApplicationsManager.exe
Nessus-3[1].2.1.1.exe
nsauditor_setup.exe

Penetration
1. Framework2-MsfCli
2. Framework2-MsfCnsole
3. Framework2-MsfUpdate
4. Framework3-MsfCli
5. Framework3-MsfConsole
6. Framework3-MsfUpdate
7. Framework3-Msfweb
8. Inguma
9. Update Miliw0rm

**Framework Version 2**
1. Framework2-MsfCli
2. Framework2-MsfConsole
3. Framework2-MsfUpdate

**Framework Version 3**
1. Framework3-MsfCli
2. Framework3-MsfConsole
3. Framework3-MsfUpdate
4. Framework3-Msfweb

miliw0rm Exploit Archive

Fast Track

Inguma
1. Nessus Server
2. ADMSnmp
3. ASP-Audit
4. Bed
5. braa
6. bunny
7. Burpsuite
8. Cisco Auditing Tool
9. Cisco Global Exploiter
10. Cisco OCS mass SCanner
11. Cisco passwd Scanner
12. Copy Router Config
13. CSRFTester
14. Curl
15. DirBuster
16. Grabber
17. Grendel Scan
18. Httprint
19. httprint_GUI
20. JBroFuzz
21. Lbd
22. List-Urls
23. Merge Router Config
24. Metacoretex
25. Mini Mysqlator
26. Nessus
27. Nikto
28. Paros Proxy
29. Pblind
30. peach
31. Ratproxy
32. SMBClient.py
33. Snmp Enum
34. Spike
35. SQLbrute
36. SQLIX
37. SQLMap
38. SQL Ninja
39. swfintruder
40. Voiper  
41. W3AF  
42. Wapiti  
43. Webscarab Lite  
44. Webshag  
45. Wfuzz  
46. WSFuzzer  
47. ZZuf  

**Cisco**  
1. Cisco Auditing Tool  
2. Cisco Global Exploiter  
3. Cisco OCS Mass Scanner  
4. Copy Router Config  
5. Merge Router Config  

**Database**  
1. DB-Generic  
2. MSSQL  

**Fuzzers**  
1. Bed  
2. bunny  
3. JBroFuzz  
4. Peach  
5. Spike  
6. Voiper  
7. WSFuzzer  
8. ZZuf  

**SMB Analysis**  
1. SMBClient.py  

**SNMP Analysis**  
1. ADMSnmp  
2. braa  
3. Snmp Enum  

**Nessus Server**

---

**Block 4: Securing during Mobility**

**Unit 1. Security in Wireless Environment**

**Unit 2. Wi-fi, Blue tooth, LAN**

Airsnarf - A rogue AP setup utility.htm  
Airsnort  
Cqure AP  
NetStumblerInstaller.exe  
WEP Cracker  
WiFi Scanners-Linux  
Wireless Hacking Tools  
aiopeek.exe  
airsnarf-0.2.tar.gz  
arppoison  
kismet  
widzv1  
wlanexpert  

**Wireless Network Analysis**

**Bluetooth**

1. Blueprint  
2. BlueSmash  
3. Btcsanner
4. HCIDump
5. Minicom
6. obexFtp
7. Ussp-Push

**Wi-Fi**
1. All
   * .Aircrack -ng (Sedulity OS EH Edition)
   * .Airmon-ng (Sedulity OS EH Edition)
   * .Airodump-ng (Sedulity OS EH Edition)
   * .AirSnarf (Sedulity OS EH Edition)
   * .ASLEAP (Sedulity OS EH Edition)
   * .Cowpatty (Sedulity OS EH Edition)
   * .Genpmk (Sedulity OS EH Edition)
   * .Kismet (Sedulity OS EH Edition)
   * .Mackchanger (Sedulity OS EH Edition)
   * .WEPbuster (Sedulity OS EH Edition)
2. Cracking
   * .Aircrack -ng (Sedulity OS EH Edition)
   * .Airmon-ng (Sedulity OS EH Edition)
   * .Airodump-ng (Sedulity OS EH Edition)
   * .AirSnarf (Sedulity OS EH Edition)
   * .ASLEAP (Sedulity OS EH Edition)
   * .Cowpatty (Sedulity OS EH Edition)
   * .Genpmk (Sedulity OS EH Edition)
   * .Kismet (Sedulity OS EH Edition)
   * .WEPbuster (Sedulity OS EH Edition)

**Unit 3. Digital Incident Response**

**Unit 4. Industry Perspective**

**Course 3: Information Technology Security – (4 Credits-Theory, Compulsory)**

**Block 1: W3C Compliance**

- **Unit 1. Introduction to W3C** Theory
- **Unit 2. Recommendations and certifications of W3C** Theory
- **Unit 3. W3C Standards and Practices** Theory
- **Unit 4. How do we Improve Internet Privacy using W3C** Theory
cynthia.exe

**Block 2: Introduction to ISO 27000**

- **Unit 1. Need of Certification** Theory
- **Unit 2. ISO/IEC 27000 family of Information Security Management Systems (ISMS) standards** Theory
- **Unit 3. Cyber Security Standards** Theory
- **Unit 4. Employee perspective of ISO 27000** Theory

**Block 3: Information Technology Act**

- **Unit 1. Introduction to Information Technology Amendment Act 2008 (Unique ID (UID), Limitations of Information Technology Amendment Act 2008)** Theory
- **Unit 2. Legal Implications of Personal Security** Theory
- **Unit 3. Common Cyber Crimes and Government Laws and Rules in Information security** Theory
Course 4: Server Security (6 Credits (1 Credit-Theory and 5 Credit-Practical), Compulsory)

Block 1: Email Security
Unit 1. Email Servers
- PostFix
- IceWarp Mail Server
- Courier mail server
- Eudora WorldMail Server
- Dovecot
- WebEasyMail
- Rockliffe
- IMail Server

Unit 2. Email Forgery and Spamming
- 65Advanced Stealth Email Redirector.zip
- aep.zip
- Email_Spider_Easy.zip
- empasrec.zip
- freesmtph.zip
- mailpv.zip
- SECRET_INSTALL.EXE
- smtpserver.exe

Unit 3. Password Attack Vectors
- Yahoo Messenger Archive Recovery Software.exe
- MSN Explorer Password Recovery Software.exe
- Nucleus-MSN-Password.exe

Unit 4. Account Security

Block 2: Windows Security

Unit 1. Windows System Architecture

Unit 2. Windows System Security

Unit 3. Hacking Windows
- ADS Streaming Utility
- ADS Visual Detector_DEMO
- ADS Visual Detector_DEMO.zip
- Antispector
- auditpol.exe
- browselist.exe
- c2myazz
- Capture LM Manager Password
- cat.exe
- Change_NT-2000_Passwords
- cmdlog
- cp.exe
- Crash on Demand.exe
- dumpel.exe
- efsview.exe
- elsave
- EvidenceEliminator.exe
- foundstone_tools
- FU_Rootkit
- getadmin
HiddenFileDetectorSetup
Hide Folders XP
hk
hydan-0.10.tar
Invisible Folders.exe
Invisible Secrets.exe
john-16w
kerbcrack
lc4setup.exe
lc5setup.exe
legion
lns.exe
makestrm.exe
md5sum.exe
Merge Streams
nbname.cpp
ntdeputy
NTFS and ADS.htm
ntinfoscan.exe
NTLM Authentication.ppt
Nt_rootkit0.40
Offline NT Password Resetter
psexec
pwdump2
pwdump3v2
remoxec
RightClickHide
Rootkit Detector V0.3 for windows
rootkithunter-1.00RC1.tar.gz
samdump
Security side-effects of Word fields.htm
ShutDown.exe
SMB Proxy
smbgrinder

OS-Fingerprinting
1.5nmap (Sedulity OS EH Edition)
2.Autoscan (Sedulity OS EH Edition)
3.Nmap (Sedulity OS EH Edition)
4.onesixtyone (Sedulity OS EH Edition)
5.p0f (Sedulity OS EH Edition)
6.Protos (Sedulity OS EH Edition)
7.sslscan (Sedulity OS EH Edition)
8.Xprobe2 (Sedulity OS EH Edition)
9.Zenmap (Sedulity OS EH Edition)

Password Attacks
1.Password offline Attacks
   *.bkhive (Sedulity OS EH Edition)
   *.john (Sedulity OS EH Edition)
   *.samdump2 (Sedulity OS EH Edition)
   *.sqlpat (Sedulity OS EH Edition)
   *.wyd (Sedulity OS EH Edition)

Block 3: Linux Security

Unit 1. Linux System Architecture

Unit 2. Linux System Security

Theory
Unit 3. Hacking Linux
7350nxt-v3.tar.gz
9x.cgi.zip
ADM-spoof-NEW.tgz
anonirc.c
boscript-0_2.tar.tar
bsd-rdist.c
cctt-0.1.7.tar.gz
cgiscan2.c
cheops-0_55.tar.tar
cold-1_0_10.tgz
cops_104.tar.z
crack5_0.tar.gz
cracklib25_small.tar.z
crontab_backdoor.sh
dipexploitlinux.c
Distributed John.tgz
dtk-0_7.tar
ethereal-0_5_0.tar.tar
fakebo-032.tgz
Firebird 1.0.2 FreeBSD 4.7-RELEASE local root exploit.htm
gammaprog150.tgz
hackunix.zip
holelist.txt
hping2_v1.5.pdf
HP-UX B11.11 -usr-bin-ct local format string Root Exploit.htm
hunt-1_0.tgz
ibnc2_0a.tar
index.html
install.txt
Intel PXE Exploit in RedHat 8.txt
inv.c
ipbomb.c
ipgrab-0_6.tar.tar
ipsend2_1a.tar.tar
ipspoof_script.zip
ircbn.c
jizz.c
jizz.sh
john-1.6.34.tar.gz
john-1_6.tar.tar
libpcap-0_4.tar.tar
Linux 2.4.20 kernel decode_fh Denial of Service Exploit.htm
Linux Basic Commands.pdf
Linux eXtremail 1.5.x Remote Format Strings Exploit.htm
linux.txt
logwatch-1_5_1.tar.tar
lrk4readme.txt
mailbseq.c
Mandrake Linux 8.2 -usr-mail local exploit (d86mail.pl).htm
merlin.tar.gz
mflash.c
modify_ldt_exploit.c
mountexp.c
nessus-unstable-120198.tgz
nfsbug.c
Block 4: Webserver Security

Unit 1. Understanding Web Technologies

Unit 2. Web Application Attacks
32 Bit IP Resolver
Automatic-Printing-in-IE Vulnerability.htm
Brute Force Attack Estimator.xls
Form Bookmarklets.url
Form Bookmarks.htm
Generate Unicode Strings.htm
Generate Xss Exploit
HTTP File Stealing
HelpMe2.pl
IE Cache Extractor
IEEN
IISSHACK.doc
Running this page will crash IE.htm
WinDNSSpoof
hacking web servers
http traffic monitor
ieflaw
iehist-win32-0_0_1.zip
jad
lynx
monkeyshell.tar.gz
Web Analysis
1. ASP-Audit (Sedulity OS EH Edition)
2. Burpsuite (Sedulity OS EH Edition)
3. CSRPTester (Sedulity OS EH Edition)
4. Curl (Sedulity OS EH Edition)
5. DirBuster (Sedulity OS EH Edition)
4. Grabber
5. Grendel scan (Sedulity OS EH Edition)
6. Httprint (Sedulity OS EH Edition)
7. Httprint_GUI (Sedulity OS EH Edition)
8. Lbd (Sedulity OS EH Edition)
9. List-Urls (Sedulity OS EH Edition)
10. Mini Mysqltator (Sedulity OS EH Edition)
11. Nikto (Sedulity OS EH Edition)
12. Paros Proxy (Sedulity OS EH Edition)
13. Ratproxy (Sedulity OS EH Edition)
14. Swfintruder (Sedulity OS EH Edition)
15. W3AF (Sedulity OS EH Edition)
16. Wapti (Sedulity OS EH Edition)
17. Webshag (Sedulity OS EH Edition)
18. Wfuzz
19. ZZuff (Sedulity OS EH Edition)
20. Webscarb Lite (Sedulity OS EH Edition)
Nessus Server (Sedulity OS EH Edition)
Nessus (Sedulity OS EH Edition)

Block 5: Wireless Network Security
Unit 1. Wireless Network Concepts

Unit 2. Wireless Attacks
Airsnarf - A rogue AP setup utility.htm
Airsnort
Cqure AP
NetStumblerInstaller.exe
WEPCrack
WiFiScanner-Linux
Wireless Hacking Tools
airopeek.exe
airsnarf-0.2.tar.gz
arppoison
kismet
widzv1
wlanexpert

Wi-Fi
1. All
   *.Aircrack -ng (Sedulity OS EH Edition)
   *.Airmon-ng (Sedulity OS EH Edition)
   *.Airodump-ng (Sedulity OS EH Edition)
   *.AirSnarf (Sedulity OS EH Edition)
   *.ASLEAP (Sedulity OS EH Edition)
   *.Cowpatty (Sedulity OS EH Edition)
   *.Genpmk (Sedulity OS EH Edition)
   *.Kismet (Sedulity OS EH Edition)
   *.Mackchanger (Sedulity OS EH Edition)
Unit 3. Wireless Security Measures
Elcomsoft Wireless Security Auditor 3.2.0.395
LucidLink Home Office Edition 2.2
PW0-200 - Wireless Security Professional (WSP) Practice Test Questions 1.0
AirStop Wireless 2.4.3

Block 6: Software Security
Unit 1. Recovering Software Codes
3568_ResHack.zip
adc-0.69.zip
boomerang-linux-alpha-0.3.tar.gz
boomerang-win32-alpha-0.3.1.zip
hw32v601.exe
idademo54.exe
PE.Explorer_setup.exe
PE.Explorer_setup.zip
spices.zip
spicesdc.zip

Unit 2. Understanding Software Code

Unit 3. Developing Software Patches and Code
FASM148.ZIP
fasmw148-090.zip
WDASM89.ZIP

3. The Institute is required to furnish the attached proforma for establishment as an IGNOU programme study centre.