1. Course Contents:

Module No:	Contents	No. of Sessions	70 Marks (External Exam)
Unit I	**Digital Security.** Introduction, Types of Attacks, Digital Privacy, Online Tracking, Privacy Laws, Types of Computer Security risks ,Malware, Hacking, Pharming, Phishing, Ransom ware, Adware and Spyware, Trojan, Virus, Worms, WIFI Eavesdropping, Scare ware, Denial-Of-Service Attack, Root kits, Juice Jacking), Antivirus and Other Security solution, Password Distributed, Secure online browsing, Email Security, Social Engineering, Secure WIFI settings, Track yourself online, Cloud storage security, IOT security, Physical Security Threads.	10	15
Unit II	**Online Anonymity** Anonymous Networks, Tor Network, I2P Network, Freenet, Darknet, Anonymous OS – Tails, Secure File Sharing, VPN, Proxy Server, Connection Leak Testing, Secure Search Engine, Web Browser Privacy Configuration, Anonymous Payment.	5	10
Unit III	**Cryptography and Secure Communication** The Difference Between Encryption and Cryptography, Cryptographic Functions, Cryptographic Types, Digital Signature, The Difference Between Digital Signatures and Electronic Signatures, Cryptographic Systems Trust Models, Create a Cryptographic Key Pair Using Gpg4win/gpg4usb, Disk Encryption Using Windows BitLocker, Disk Encryption Using Open Source Tools, Multitask Encryption Tools, Attacking Cryptographic Systems, Countermeasures Against Cryptography Attacks, Securing Data in Transit, Cloud Storage Encryption, Encrypt DNS Traffic and Email Communication, Secure IM and video calls.	6	12
Unit IV	**Digital Forensics** Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Network Forensics, Mobile Forensics, Cloud Forensics. **Network security:** Handling Received Client Data over TCP Socket, Blocking and Non-Blocking Socket I/O, Application Banner Grabbing, Building an Anonymous FTP Scanner with Python, Using Ftplib to Brute Force FTP.	10	15
Unit V	**Cyber Crime Issues and Investigation** Unauthorized Access, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law	10	18

	Enforcement Roles and Responses, Investigation Tools, e-Discovery, EDRM Model, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking		

2. Pedagogy:

- ICT enabled Classroom teaching
- Case study
- Practical / live assignment
- Interactive class room discussions

3. Evaluation:

Students shall be evaluated on the following components:

A	**Internal Evaluation**	**(Total - 20 Marks)**
	• Continuous Evaluation Component	10 marks
	• Class Presence & Participation	10 marks
B	**Mid-Semester examination**	**(30 Marks)**
C	**End –Semester Examination(Theory)**	**(70 Marks)**
D	**End –Semester Examination(Practical/Viva)**	**(30 Marks)**

4. Text Book:

No.	Author	Name of the Book	Publisher
1	Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short	Cybersecurity Essentials	ISBN: 978-1-119-36239-5. SYBEX
2	Digital Forensics with Open Source Tools	Cory Altheide, Harlan Carvey	ISBN: 978-1-59749-586-8, Elsevier, Syngress.

5. Reference Books:

No.	Author	Name of the Book	Publisher
1	Dafydd Stuttard, The Web Application Hacker′s	Handbook: Finding and Exploiting Security Flaws	Paperback – Wiley, 2nd Edition
2	James Graham, Richar Howard,Ryan Olson	"Cyber Security Essentials",	CRC Press, Tailor and Francis Group, 2011
3	Nelson Phillips, Enfinger Steuart,	"Computer Forensics and Investigations"	Cengage Learning, New Delhi, 2009.
4	Peter Wayner, Morgan Kaufmann	"Disappearing Cryptography – Information Hiding: Steganography & Watermarking"	Publishers, New York, 2002.
5	Kenneth J. KnappIGI Global	"Cyber Security and Global Information Assurance ,Threat Analysis and Response Solutions",	2009.

Practical/ Tools:

1) Mike Shema, Anti-Hacker Tool Kit (Indian Edition), Mc Graw Hill.

2) Christian Martorella , Learning Python Web Penetration Testing,PAKT

3) Vijay Kumar Velu, Mastering Kali Linux for Advanced Penetration Testing, PAKT, Book 2017

4) Nipun Jaswal, Mastering Metasploit, Take your penetration testing and IT security skills to a whole new level with the secrets of Metasploit, 3rd Edition Paperback – Import, 28 May 2018 by

5) Gilberto Najera-Gutierrez, Juned Ahmed Ansari, Web Penetration Testing with Kali Linux - PAKT, Third Edition February 2018

Appendix-A

Sample Practical List

Part I - Commands

1. Study of following network emulators:
    a) WHOIS Search
    b) Whois CLI Command
    c) Nslookup
    d) Host
    e) Ping
    f) Traceroute
    g) Netstat
    h) Tcpdump and Windump
2. Create a malicious program that is (Atleast one program):
    a) Virus
    b) Worm
    c) Trojan
    d) Dropper
3. TCP / UDP connectivity using Netcat
4. TCP scanning using NMAP.
5. Port scanning using NMAP.
6. TCP / UDP connectivity using Netcat.

Part II - Exploits

7. Exploit Web Application Security using DVWA.

Command Execution

- SQL Injection
- SQL Injection (Blind)
- File Inclusion
- File Upload
- Insecure CAPTCHA
- Brute Force

- CSRF
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript

8. Exploit Web application Security using DVWA

Automated SQL injection with SqlMap.

Part III - Forensics

9. Perform a forensic analysis through autopsy sleuth kit.
10. Perform forensic analysis through helix.
11. Study of Forensic Tools (Study any TWO)
    - Password Clearing
    - File Recovery
    - Data Hiding Techniques
    - Steganography
    - Checksum
    - Hiren's BootCD