

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Network Security and Forensics
Course Code:	2ET2070107T
Pre-requisite Course:	Basic knowledge about computer networks and troubleshooting of network systems

Course Objectives: After successful completion of the course, student will be able to

1. This course aims to provide advanced background on relevant computer networking topics to have a comprehensive and deep knowledge in computer networks.
2. This course will cover the concept of security, types of attack experienced, encryption and authentication for deal with attacks, what are Network Perimeter Security, Access Control Lists and Virtual Private Networks.
3. This course aims to provide advanced background on relevant computer networking topics to have a comprehensive and deep knowledge in computer networks.
4. To apply algorithms used for secure transactions in real world applications
5. Combines both the technical expertise and the knowledge required to investigate, detect and prevent network crimes.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weight age (%)
1	Networking Basics: Familiarization of Networking tools like traceroute, netstat, nslookup, nc, arp etc, Configuring servers like samba and SMTP in linux, Socket Programming with python;	09	20
2	Techniques for Network Protection: Firewalls, packet filter and stateful firewalls, application aware firewalls, personal firewalls-iptables, Proxies, NAT, Intrusion Detection System-Snort, Signature and Anomaly based detection, Honeypots and Honeynets, Network Log management-syslog or SPLUNK; RBAC: Role mining; Network reconnaissance-Nmap and vulnerability audits-openVAS; DNS-Dig tool: DNS based attacks, Phishing-DNSTwist, DNSSEC-DS and NSEC records;	09	20
3	Network based malware attacks: Remote access Trojan-Poison Ivy and Domain name generation algorithm based Botnets; LAN attacks: ARP Cache poisoning, MAC flooding, Man in the middle attacks, Port Stealing, DHCP attacks, VLAN hopping; Network Sniffing-Wireshark and Password Cracking-John the Ripper, tcpdump, windump;	09	20
4	Secure Network Communication: SCP, SSH, SSL3.0, TLS 1.2, STARTTLS, IPSec, VPN and Secure HTTP; Understanding the dark web, TOR traffic, Attacks on SSL/TLS: SSL stripping, Drown and Poodle attack; Encrypting and Signing Emails: PGP- GPG/openPGP, DKIM and SPF; Single Sign On (SSO) OAUTH and OPENID; Network packet creation and Manipulation using scapy and dpkt libraries; SDN Security.	09	20

5	Forensic Tools and Report Generation: Recovery of Deleted files in windows and Unix, Analyzing network traffic, sniffers, Ethical Hacking, Hardware forensic tools like Port scanning and vulnerability assessment tools like Nmap, Netscan etc. Password recovery (tools like John the ripper, L0phtcrack, and THC-Hydra), Mobile forensic tools and analysis of called data record Template for computer forensic reports	09	20
---	---	----	----

Text Books:

1. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson edition, 2016.
2. Vincent J. Nestler et. al, Principles of computer security Lab Manual, 4th Edition, McGraw-Hill, 2014

Reference Books:

1. Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence by William Oettinger , Pckt Publishers
2. John Sammons, the Basics of Digital Forensics, Elsevier, 2014.
3. Behrouz A. Forouzan, Cryptography & Network Security, McGraw-Hill, 2007
4. C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a Public World, 2nd Edition, Prentice Hall PTR, 2002.

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Understand various techniques for Network Protection and explore new tools and attacks in network security domain	Applying (2) / Applying (1)
COL2	Exploring DNS based attacks and DNSSEC	Applying (2) / Applying (3)
COL3	Familiarize the LAN based attacks and its mitigations	Applying (4)
COL4	Exploring Secure Network Communication protocols and attacks	Applying (5)
COL5	Knowledge on network forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation	Applying (1) / Applying (5)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	H	H	H			L							H	M
CLO2	H	M	H	H	H			L				L			H	M
CLO3	H	M	M	H	H			L							M	M
CLO4	M	M	M	H	H			L				L			M	M
CLO5	M	M	M	H				L				L			M	M

H: High, M: Medium, L: Low