Introduction to Cyber Security
(Free Elective-II)

COURSE CODE: 15FE1114

L	T	P	C
1	0	0	1

COURSE OUTCOMES:

At the end of the course the student shall be able to

CO1: Understand the basics of network and security.
CO2: Apply Windows Security Principles.
CO3: Explore Attacker techniques.
CO4: Understand Fraud techniques and threat infra structure.
CO5: Analyze exploitation techniques.

UNIT-I **(4 Lectures)**

Network and Security Concepts:

Information Assurance Fundamentals- Authentication, Authorization, Nonrepudiation, Confidentiality, Integrity, Availability. Basic Cryptography, Symmetric Encryption, Public Key Encryption, Firewalls, Virtualization.

UNIT-II **(3 Lectures)**

Microsoft Windows Security Principles:

Windows Tokens, Window Messaging, Windows Program Execution, The Windows Firewall.

UNIT-III **(3 Lectures)**

Attacker Techniques and motivations:

How Hackers Cover Their Tracks (Antiforensics)**,** Tunneling Techniques- HTTP, DNS, ICMP, Intermediaries, Steganography and Other Concepts, Detection and Prevention

UNIT-IV **(4 Lectures)**

Fraud Techniques and Threat Infrastructure:

Phishing, Smishing, Vishing, and Mobile, Malicious Code, Rogue Antivirus, Click Fraud, Botnets, Fast-Flux, Advanced Fast-Flux.

UNIT-V **(4 Lectures)**

Exploitation Techniques to Gain a Foothold:

Shellcode, Integer Overflow Vulnerabilities, Stack-Based Buffer Overflows, Format String Vulnerabilities, SQL Injection, Malicious PDF Files, Race Conditions.

Text Books:

1. James Graham, Richard Howard, Ryan Olson "CYBER SECURITY ESSENTIALS", CRC Press, Taylor & Francis Group, International Standard Book Number-13: 978-1-4398-5126-5,2011.

References:

1. Martti Lehto, Pekka Neittaanmäki, " Cyber Security: Analytics, Technology and Automation", Springer-Intelligent Systems, Control and Automation: Science and Engineering-Volume 78, 2015.

WEB REFERENCES:

1. https://www.coursera.org/learn/intro-cyber-security-business