CYBER SECURITY ESSENTIALS

COURSE OBJECTIVES

LTPC 3003

- To make the students understand the basic cyber attacks and vulnerabilities
- To understand the principles, practices and processes involved in cybersecurity
principles
To familiarize system and network defense
To expose asset management and risk management and the governance and
compliance.
-
- **Cyber Security Fundamentals**
Network and Security Concepts – Information assurance Fundamentals – basic cryptography – symmetric encryption – Domain Name System (DNS) – Computer networks – Firewalls – virtualization

Attacker Techniques and Motivation

Antiforensics – proxies – types of proxies – detecting the use of proxies – tunnelling techniques – detection and prevention – phishing, smishing, vishing and malicious code – rogue antivirus – click fraud – Threat infrastructure: Botnets – fast flux

Exploitation

Shellcode – integer overflow vulnerabilities – stack-based buffer overflows – SQL injection – malicious PDFs – Race conditions – Web exploit tools – brute force and dictionary attacks – cross site scripting – Social engineering.

Malicious code

Self-repeating malicious code – worms – viruses – obfuscation – VM obfuscation – persistent software techniques – spyware

Assets & Risk Management

Memory forensics – honeypots – malicious code naming – automated malicious code analysis – Asset and Risk management – risk assessment – Security controls.

COURSE OUTCOMES

After the completion of this course, students will be able to: • Explain firewalls and basic crypto systems

• Explore different attacks, phishing, smishing and vishing.
• Analyse and implement methods to counterattack cyberattacks. • Get exposed to asset and risk management.

TEXT BOOKS

Total: 45 hours

1. James Graham, “Cyber security essentials”, CRC Press, Taylor & Francis Group, 2010.