

## Week 1: Introduction to Cybersecurity

Name: KASA SATYA SAMPATH KUMAR

Roll Number: 2023002939

Year: III Year

Program: B.Tech. Computer Science and Engineering

Club: HackOps – GITAM University

### 📌 Summary of Learning Content:

- Cybersecurity means protecting systems, networks, and data from digital threats like unauthorized access or cyberattacks.
- It is a multidisciplinary field with 8+ domains and 25+ subdomains including offensive, defensive, cloud, forensics, legal, and governance areas.

### 📌 Key Domains in Cybersecurity:

- Red Team (Offensive Security)
  - - Simulates real cyberattacks
  - - Includes penetration testing, exploit development, social engineering
- Blue Team (Defensive Security)
  - - Detects and responds to threats in real-time
  - - Uses SIEM, threat intelligence, incident response
- DevSecOps & Cloud Security
  - - Builds security into development pipelines
  - - Focuses on securing AWS, Azure, GCP
- GRC (Governance, Risk & Compliance)
  - - Deals with policies, risk assessments, compliance (GDPR, ISO 27001)
- Cybersecurity Law & Policy
  - - Covers data privacy laws and cybercrime regulations
- Security Awareness & Training
  - - Focuses on phishing simulations, gamified training, user education

## 📖 Subdomains & Topics

- Red Team Tools:
  - - Web app security, mobile security, social engineering, physical security
- Blue Team Tools:
  - - SOC & threat monitoring, EDR/XDR, log analysis, IAM, patch management

## 📖 Common Myths Busted:

- You don't need to be a coding expert
- Cybersecurity is not only hacking
- A specific degree isn't required
- Expensive certifications aren't necessary to start

## 📖 Platforms and Resources Mentioned:

- Training: TryHackMe, HackTheBox, PicoCTF, Pwn College, Bandit Labs, Udemy
- Bug Bounties & CTFs: HackerOne, BugCrowd, CTFtime
- Communities: Instagram, GitHub, Telegram, LinkedIn