1. Introduction of Internet

-Internet Addresses, DNS, Internet Infrastructure, World Wide Web.

2. Introduction to Cyber Crime

-Classification of cyber-crimes, reasons for commission of cyber-crimes.

3. Cyber Security Fundamentals

-Introduction to Cybersecurity Science, The Importance of Cybersecurity science, Network security concepts, Microsoft windows security principles.

4. Malware and its types

-Adware, spyware, browser hacking software, virus, worms, Trojan horse, scareware.

5. Kinds of Cyber crime

-Cyber stalking, child pornography, forgery and counterfeiting, software piracy and crime related to IPRS, phishing, vishing, computer hacking and vandalism, spamming etc

6. Authentication, Encryption, Digital signatures

7. Attackers Techniques and Motivation

-How and why attackers use proxies, Detecting the use of proxies, tunnelling techniques fraud techniques, threat infrastructures.

8. Setting up your virtual lab

-VMware, Introduction to Kali Linux/ParrotOS, programming, Exploitation using Metasploit Framework.

9. Malicious Code

-Self-replicating Malicious code, evading detection and elevating privileges, Stealing information and Exploitation.

10. Practical's