Ethical Hacking and Cyber Security Syllabus	
Session 1: Network Concepts (CompTIA)	
➢ What is Network?, Network Topology, Internet Working, Domain Name, Server	➢ Ports and Types of Ports, Ethernet, Infrastructure and Design, Policies and Best Practices
➢ Internet Protocol, IPV4, IPV6	➢ Introduction to Web Browser
Session 2: Ethical Hacking & Cyber Security Overview	
➢ Cybercrime scenario in India and worldwide, Short description about hacking vs. Ethical Hacking	➢ Skill Profile of a Hacker, Some Famous Hackers and Groups, Types of Hackers
➢ Advantages and Disadvantages of Cyber world	➢ Skills required for an Ethical Hacker
Session 3: Overview of Cyber Law	
➢ Introduction to Cyber Law, Cyber Laws Indian	➢ Technical Aspect of Indian Cyber Law, IT ACT 2000 and 2008, Internet Crimes and Frauds
➢ Cyber Law Cases in India, Organization Under Cyber Laws	➢ Advantages of Cyber Laws
Session 4: Computer Virtualization Technology and Lab Setup	
➢ Need and Advantages of Virtualization, Requirements for virtualization	➢ Creating Virtual Machines and optimization performance
➢ Installing OS (Windows and Linux) On Virtual Machines	➢ Virtual Networking what and why?
Session 5: Information Gathering	
➢ What is Information Gathering & Why Hackers Need This?	➢ Types of Information Gathering, Information Gathering Using Websites, Information Gathering Using Software's
➢ Search Engines – Smart way of Information Gathering, Ping, Who-is Lookup	➢ People Search, DNS Lookup, Benefits of Foot Printing
Session 6: Windows, Linux hacking and security	
➢ Introduction Windows Security, User Accounts Security, Attacks and countermeasure	➢ Hacking into System by Changing Passwords, Getting Access to System by Elevating Privileges
➢ Finding Out the Passwords of Windows	➢ By Passing the Windows Security
Session 7	
➢ Data Recovery	➢ Steganography and Cryptography
Session 8: Cloud	
➢ Cloud Computing Concepts, Cloud Reference Architecture	➢ Security Concepts relevant to Cloud Computing
➢ The Design Principles of Secure Cloud Computing	➢ Trusted Cloud Services
Session 9	
➢ Fake Calling and SMS	➢ Use of Mobile in Hacking
➢ Hidden Function of Mobile	➢ Backdoor Attack
Session 10: Denial of Service Attack (DOS- Attack)	
➢ What is a Denial of Service Attack?	➢ What is Distributed Denial of Service Attacks?
➢ DoS Attack Techniques	➢ Detail Study on DoS Attack Tools
Session 11: Hacking by viruses, Trojans, Key Loggers	
➢ What is Viruses? What is Trojan?	➢ Trojans/Viruses Attack
➢ Different way a Trojan Can Get into a System	➢ How Attacker Bypass Your Antivirus By Trojans
Session 12: VPN Technology	

➢ Proxy and Types of Proxies	➢ Why Hackers Use Proxy?
➢ How to Hide IP Address While Chatting?	➢ How to Open Block Website in College/Companies?
➢ Advantage and Disadvantages of Proxy	➢ What is VPN? Why we use VPN?
➢ Advantage and Disadvantage of VPN	➢ Free VPN
Session 13: Google Hacking and Google Hacking Database	
➢ Introduction and Working of Search Engines, List of Common Search Engines on Web	➢ Comparing and Choosing Best Search Engine, Google For Hacking Search Engines
➢ Finding Admin Pages and Weakness in Site	➢ Security against Search Engine Hacking
Session 14: Email/Social Sites Hacking and Security issues	
➢ Analysis Email Attacks (Live Demo) Manually and Automatic	➢ Cookies Stealing (Session Hijacking) of All Big Mail Servers
➢ Phishing Attacks (Normal & Advanced), Analyzing Fake & Real Profiles & Email Accounts	➢ Fake Mailing Attack, Email & Fake Profile Tracing, Facebook Phishing Attacks
➢ Facebook Account Security with Email	➢ Facebook Account Security with SMS Notification
Session 15: SQL Injection	
➢ SQL Injection Attacks	➢ How Web Applications Work
➢ SQL Injection Detection, Types of SQL Injection	➢ How to Defend Against SQL Injection Attacks??
Session 16: Wireless Hacking	
➢ Wireless Standards, Common Vulnerabilities in Wireless Devices	➢ Encryption Standards Used in Wi-Fi, WEP Cracking
➢ WPA/WPA2 Cracking, WPS Cracking	➢ Solve Security Challenges
Session 17: Linux Training	
➢ What is Linux & How to operate this OS	➢ Use of Linux, Function in Linux, Terminal Function
➢ Site Cloning, Network Scanning, Security	➢ Wi-Fi Jammer, Armitage, NMAP and many more hacking tools
Session 18: Security and Risk Management	
➢ Understand and apply concepts of Confidentiality, Integrity and Availability	➢ Apply Security Governance Principles through compliance, Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
➢ Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines	➢ Understand Business Continuity Requirements, Contribute to Personnel Security Policies
➢ Understand and Apply Risk Management Concepts, Understand and Apply Threat Modelling	➢ Integrate Security Risk Considerations into Acquisitions Strategy and Practice, Establish and Manage Security Education Training and Awareness
Session 19: Security Architecture Engineering	
➢ Understand the engineering life cycle and apply security design principles	➢ Understand the fundamental concepts of security models, Select controls based upon systems security requirements
➢ Understand the security capabilities of information systems, Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements	➢ Assess and mitigate the vulnerabilities in Web-based systems, Assess and mitigate the vulnerabilities in Mobile Systems, Assess and mitigate the vulnerabilities in Embedded devices
➢ Apply Cryptography, Implement Facility Security Controls	➢ Wiring Closets/Intermediate distribution facility
Session 20: Communication and Network Security	
➢ Apply Secure Design Principles in Network	➢ Implement Secure Communication Channels

Architecture, Securing Network Components	according to design
Session 21: Identity and Access Management (IAM)	
➢ Control Physical and Logical Access to Assets, Manage Identification and Authentication of People and Devices	➢ Integrate Identity as a Service (IDaaS), Integrate Third-Party Identity Services, Implement and Manage Authorization Mechanisms
➢ Prevent or Mitigate Access Control Attacks	➢ Manage and Identity and Access Provisioning Life Cycle
Session 22: Audit	
➢ The Process of Auditing Information Systems	➢ Governance and Management of IT
➢ Protection of Information Assets	
Session 23: Security Assessment and Testing	
➢ Design and Validate Assessment, Test and Audit Strategies	➢ Conduct Security Control Testing
➢ Collect Security Process Data	➢ Conduct or Facilitate Security Audits
Session 24: Security, Cyber Crime Case Study	
➢ Facebook/mail Account Security, Website Security, Wi-Fi Security, WhatsApp Security	➢ Android Phone Security, Introduction to Cyber Crime and Investigation, Types of cyber crimes
➢ Investigation Rules	➢ More Case Study based on Cyber Crime