# Ethical Hacking Essentials with Kali Linux

### Class 1: Introduction to Kali Linux and Basic Linux Usage Part-1

- Overview of Kali Linux distribution
- Installation and setup basics
- Command line interface (CLI) navigation
- Linux Shells and Terminal
- Linux Directory Structure
- Linux file and directory types
- Basic commands: `cd`, `ls`, `mkdir`, `pwd`
- File manipulation: `cp`, `mv`, `rm`

### Class-2: Kali Linux and Basic Linux Usage Part-2

- Linux Text Processing Tools
- Manipulating linux Text Files, Save, Delete, Overwrite
- Linux User Creation and Deletion
- Overview of Passwd, Shadow files
- Working with Help and Manual command
- Basic System Information gathering Commands

### Class-3: Networking Basics Part-1

- Introduction to Computer Networks
- Types of Networks LAN, WAN, MAN, PAN
- Network Topologies: Bus, Star, Ring, Mesh
- Network Devices: Routers, Switches, Hubs, and Bridges

### Class-4: Networking Basics Part-2

- OSI Model: Layers and Functions
- IP Addressing and Classes
- Subnet Masks and Subnetting
- CIDR Notation

- Network Protocols: HTTP/HTTPS, FTP, SMTP, and DNS
- DHCP and NAT

### Class 5: Introduction to Cyber Security & Ethical Hacking

- What is Cyber Security
- What is Ethical Hacking
- Hackers Types / Classes
- Essential Terminologies / Languages of Hacking
- Hacking Methodologies (5 Phases)
- Key concepts: confidentiality, integrity, availability (CIA triad)
- Types of Cyber Attacks: Phishing, Ransomware, DDoS, and Insider Threats
- Modes of Ethical Hacking
- Types of Security Testing

### Class-6: Information Gathering

- Footprinting & Reconnaissance
- Passive vs Active Reconnaissance
- Tools: `nslookup`, `dig`, `whois`, `ping`, `traceroute`
- Google Hacking Basics and Advanced Search Operators
- Introduction to OSINT (Open-Source Intelligence) and its importance
- Identifying email addresses and associated information
- DNS Enumeration and Subdomain Discovery
- Introduction to network mapping

### Class-7: Scanning and Enumeration Part-1

- Introduction to Network Scanning
- Scanning Tools
- Host Discovery
- Types of Scanning: Network, Port, and Vulnerability Scanning
- Port Scanning Techniques: SYN Scan, ACK Scan, and UDP Scan
- Using `nmap` for Port Scanning and Service Enumeration
- Understanding the Results of an `nmap` Scan

### Class-8: Scanning and Enumeration Part-2

- Banner grabbing and fingerprinting services
- Network Discovery using Tools like `netdiscover` and `arp-scan`
- OS detection and Version Enumeration
- Understanding vulnerability scanning tools: `Nikto`
- Identifying Open Ports and Associated Vulnerabilities
- Detecting live hosts and mapping network architecture

### Class-9: System Hacking

- System Hacking Methodologies and Phases
- Techniques for Gaining Initial Access to a System
- Password Cracking Basics: Dictionary, Brute Force, and Rainbow Table Attacks
- Using Tools like `Hydra`, `John the Ripper` for Password Cracking
- Exploiting System Vulnerabilities using `Metasploit`
- Introduction to keyloggers and how they are used
- Gaining Remote Access via Remote Desktop Protocol (RDP) and SSH
- Introduction to Buffer Overflow Attacks
- Best practices for securing systems against hacking attempts

### Class-10: Malware Threats

- Introduction to Malware Concepts
- Types of Malware: Viruses, Worms, Trojans, Ransomware, Spyware, and Adware
- Understanding the Lifecycle of Malware
- Methods of Malware Propagation (e.g., Phishing Emails, Drive-by Downloads, Infected USBs)
- Introduction to Ransomware and Recent Ransomware Attacks
- Basics of Malware Analysis: Static vs Dynamic Analysis
- Detecting and Defending against malware using antivirus software
- Analyzing Malware Behavior in a Controlled Environment (Sandboxing)
- Case studies of Recent malware attacks (e.g., WannaCry, Stuxnet)
- Basics of Anti-Malware Strategies: Software Updates, Firewalls, and Safe browsing Practices
- Best practices for Protecting Against Malware (e.g., Regular Backups and Endpoint Protection)

### Class-11: Sniffing

- Introduction to Sniffing: Definition & How does it work
- Types of Sniffing: Active vs Passive Sniffing
- Popular Sniffing Tool overview (Wireshark, tcpdump, Ettercap)
- Susceptible Protocols: IMAP, SMTP, FTP, TFTP, POP3
- Sniffing Techniques: MAC Attacks
- Sniffing Techniques: ARP Poisoning
- Sniffing Techniques: DHCP Starvation
- Sniffing Techniques: DNS Poisoning
- Spoofing Attacks
- Defending and Countermeasures Techniques Against Sniffing

### Class-12: Social Engineering

- Introduction to Social Engineering Concepts
- Social Engineering Phases, Principles & Behaviors
- Common Targets of Social Engineering
- Social Engineering Attacks: Human Based
- Social Engineering Attacks: Computer Based
- Social Engineering Attacks: Mobile-Based Attacks
- Insider Threats & Identity Theft
- Social Engineering Countermeasures

### Class-13: Web Application Security

- Introduction to Web Application Security
- OWASP Top 10 vulnerabilities
- Web Application Attacks: SQL Injection
- Web Application Attacks: Broken Authentication
- Web Application Attacks: XSS (Cross Site Scripting)
- Web Application Attacks: CSRF (Cross Site Request Forgery)
- Web Application Attacks: Command Injection
- Web Application Attacks: RFI & LFI

- Web Application Attacks: Directory Traversal
- Counter Measures &Security Best Practices for Web Applications

### Class-14: Hacking Wireless Networks

- Wireless Security Concepts and Terminologies
- Types of Wireless Networks: WEP, WPA, WPA2, WPA3
- Wireless Hacking: Threat, Network DIscovery, Wifi Adapter
- Wireless Attacks: Rogue AP, Evil-Twin, Honeypot, DoS, Mac Filter
- Wireless Cracking Attacks: WEP, WPA/WPA2 Cracking
- Tools: Aircrack-ng, Airmon-ng, Wifite, Kismet
- Wireless Sniffing and Eavesdropping
- Wireless Hacking Countermeasures

### Class-15: Denial of Service

- Introduction to DoS & DDoS
- Botnets
- DoS / DDoS Attack Techniques
- Three Types of DoS / DDoS: Volumetric, Protocol, Application Layer
- Attack Explanation: IP Fragmentation, TCP State-Exhaustion
- Attack Explanation: SYN, SYN Flood (half Open)
- Attack Explanation: ICMP Flood, Smurf Attack
- DoS & DDoS Attack Tools
- Mitigations

### Class-16: Cryptography & Closing Notes

- Introduction to Cryptography
- Basic Terms and Concepts
- Symmetric vs Asymmetric Encryption
- Public Key Infrastructure (PKI)
- Hashes
- Cryptographic Attacks
- Career Opportunities in Cyber Security

- Building a Cyber Security Career Path
- Certifications and Qualifications

------------------------------------------------ Prepared by Sauradip Roy ------------------------------------------------------