

Assume you are expert in kali linux and software tester what topics to learn in kali linux as a SDET. Provide all the topics from basics to advanced, not leaving any.

As an **SDET (Software Development Engineer in Test)** using **Kali Linux**, you should focus on mastering both **penetration testing** and **security automation** to enhance your testing capabilities. Below is a **comprehensive roadmap**, covering everything from the **basics** to **advanced** topics in Kali Linux that are relevant for an SDET.

1. Basics of Kali Linux

✓ Introduction to Kali Linux

- What is Kali Linux?
- Installation (VirtualBox, VMware, Dual Boot)
- Kali Linux Architecture

✓ Linux Fundamentals

- Linux File System Hierarchy (`/`, `/etc`, `/var`, `/tmp`, `/home`, `/usr`)
- File and Directory Commands (`ls`, `cd`, `mv`, `cp`, `rm`, `find`, `locate`)
- User Management (`adduser`, `deluser`, `passwd`, `sudo`)
- Process Management (`ps`, `top`, `kill`, `htop`)
- Permissions (`chmod`, `chown`, `sudo`, `su`)
- Networking (`ifconfig`, `ip`, `netstat`, `nmap`)

✓ Shell Scripting for Automation

- Bash Scripting Basics
- Writing Automated Test Scripts in Bash
- CRON Jobs for Scheduling Tests

✓ Package Management

- APT Package Manager (`apt update`, `apt install`, `apt remove`)
- Installing Security Tools (`apt install nmap metasploit-framework`)
- Managing Repositories

✓ Networking Essentials for Security Testing

- IP Addressing and Subnetting
- TCP/IP Protocols (TCP, UDP, ICMP, ARP)
- Ports and Protocols (`netcat`, `telnet`, `ssh`, `traceroute`, `ping`)

2. Penetration Testing Essentials

✓ Network Scanning & Enumeration

- **Nmap**: Port Scanning, OS Fingerprinting
- **Netcat**: Network Exploration, Port Forwarding
- **Wireshark**: Packet Analysis
- **TCPDump**: Capturing Network Traffic

✓ Web Application Security Testing

- **Burp Suite**: Intercepting and Manipulating Requests
- **OWASP ZAP**: Automated Security Testing
- **SQL Injection Testing**
- **Cross-Site Scripting (XSS) Testing**
- **Broken Authentication Testing**

✓ Vulnerability Assessment

- **Nikto**: Web Server Scanner
- **OpenVAS**: Automated Vulnerability Scanner
- **WPSCAN**: WordPress Security Testing

✓ Exploitation Basics

- Introduction to **Metasploit Framework**
- Finding Vulnerabilities and Exploiting Them
- Writing Custom Exploits in Metasploit

✓ Wireless Network Security

- **Aircrack-ng**: Cracking Wi-Fi Passwords
- **Wifite**: Automating Wireless Attacks

✓ Social Engineering Attacks

- **Social Engineering Toolkit (SET)**
- **Phishing Campaigns & Payload Delivery**

3. Advanced Security Testing & Automation

✓ Scripting for Automated Security Testing

- Python for Security Testing (`requests`, `scapy`, `paramiko`)

- Writing Automated Scanners
- Creating Custom Exploits

✓ API Security Testing

- Testing APIs using Postman, Rest Assured (Java)
- JWT Token Security Testing
- API Rate Limiting & Authentication Bypass

✓ Fuzzing for Security Testing

- ffuf & wfuzz: Brute Forcing Web Applications
- Radamsa & AFL: File Format Fuzzing

✓ Reverse Engineering & Malware Analysis

- Ghidra & IDA Pro: Analyzing Malware
- Strings & Hexdump: Extracting Hidden Information
- Dynamic Analysis with strace/ltrace

✓ Mobile Application Security Testing

- Drozer & Frida: Android App Testing
- Objection: iOS App Security Testing
- Reverse Engineering APK Files

✓ Cloud Security & Pentesting

- AWS & Azure Security Testing
- Scanning Cloud Environments with Pacu
- Exploiting Misconfigurations

✓ Container Security Testing

- Docker & Kubernetes Security
- KubeHound & Trivy for Container Security
- Escaping Docker Containers

4. Red Teaming & Advanced Exploitation

✓ Active Directory Exploitation

- BloodHound & Neo4j: AD Enumeration
- Kerberoasting & Pass-the-Hash Attacks

✓ Privilege Escalation

- Linux Privilege Escalation Scripts
- Windows Privilege Escalation (WinPEAS, Mimikatz)

✓ Bypassing Firewalls & IDS

- Evasion Techniques
- Cobalt Strike for Red Teaming

✓ Writing Custom Exploits

- Buffer Overflow Exploits
 - ROP (Return Oriented Programming) Attacks
-

5. Cybersecurity Tools & Frameworks for SDET

✓ Common Tools You Must Know

- Metasploit Framework
- Nmap & Zenmap
- Burp Suite & OWASP ZAP
- Aircrack-ng & Wireshark
- sqlmap (SQL Injection Automation)
- Gobuster & Dirb (Directory Bruteforce)

✓ Writing & Automating Security Tests in Selenium & Cypress

- Automating Security Test Cases in Selenium
- Using Cypress for Security Automation
- Writing Java-based API Security Tests with Rest Assured

✓ DevSecOps & Security Automation

- Integrating Security in CI/CD Pipelines
 - Static Code Analysis (SonarQube, Snyk)
 - Container Security in DevOps (Aqua, Trivy)
-

6. CTF (Capture The Flag) Challenges & Practical Experience

✓ Platforms to Practice Penetration Testing

- Hack The Box (HTB)
- TryHackMe
- PentesterLab
- OverTheWire (Bandit, Narnia)

✓ Bug Bounty Programs

- HackerOne & Bugcrowd
 - Finding & Reporting Security Vulnerabilities
-

Final Thoughts

As an **SDET in Kali Linux**, you will have an **edge in automation, security testing, and penetration testing**. Start by mastering **Linux basics**, move on to **penetration testing**, and then automate security testing using **Scripting, Python, API Security Testing, and CI/CD Security Integration**.

Would you like a **structured study plan** with resources for each topic? 🚀