

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? 🚀

4o

You said:

yes

ChatGPT said:

Here's a **structured study plan** to learn **Kali Linux for SDET**, covering **basics to advanced topics** with **learning resources** and a **timeline** for mastering each concept. 🚀

---



# 12-Week Kali Linux Study Plan for SDET

This plan is structured **weekly** for **3 months**. Each week focuses on specific topics, with **learning resources, hands-on tasks, and tools**.

---



## Week 1: Kali Linux Fundamentals

### **Goals:**

- ✓ Install and set up Kali Linux
- ✓ Learn basic Linux commands & file system
- ✓ Master user management & permissions

### **Hands-on Tasks:**

- ✓ Install Kali Linux (VirtualBox/VMware)
- ✓ Navigate Linux File System (`cd`, `ls`, `pwd`, `find`)
- ✓ Manage users & permissions (`chmod`, `chown`, `sudo`)

### **Learning Resources:**

- Kali Linux Installation Guide
  - [Linux Command Line Basics](#)
  - TryHackMe - Linux Fundamentals
- 

## **Week 2: Shell Scripting & Automation**

### **Goals:**

- ✓ Write basic Bash scripts for automation
- ✓ Schedule cron jobs for periodic security tests
- ✓ Automate basic penetration tests

### **Hands-on Tasks:**

- ✓ Create a Bash script to list all open ports (`netstat -tulnp`)
- ✓ Schedule a cron job to check active users (`who`) every hour

### **Learning Resources:**

- [Bash Scripting Guide](#)
  - Automating Tasks with Cron
- 

## **Week 3: Networking & Web Security Basics**



### **Goals:**

- ✓ Understand networking concepts (IP, TCP, UDP, DNS)
- ✓ Learn network scanning with Nmap
- ✓ Capture network packets with Wireshark

### **Hands-on Tasks:**

- ✓ Scan your own system using Nmap (`nmap -A localhost`)
- ✓ Capture network traffic using Wireshark

### **Learning Resources:**

- Nmap Scanning Cheat Sheet
  - Wireshark Tutorial
- 

## **Week 4: Web Application Security Testing**

### **Goals:**

- ✓ Test websites for vulnerabilities
- ✓ Learn Burp Suite & OWASP ZAP
- ✓ Perform SQL Injection & XSS testing

### **Hands-on Tasks:**

- ✓ Use Burp Suite to intercept login requests
- ✓ Perform SQL Injection on a test website (TryHackMe)

### **Learning Resources:**

- Burp Suite Basics
  - OWASP ZAP Guide
  - TryHackMe - OWASP Top 10
- 

## **Week 5: API Security Testing**

### **Goals:**

- ✓ Understand API security vulnerabilities

- ✓ Test APIs with Postman & Rest Assured
- ✓ Learn JWT token security

#### **Hands-on Tasks:**

- ✓ Perform API security testing using Postman
- ✓ Automate API security tests in Java (Rest Assured)

#### **Learning Resources:**

- API Security Fundamentals
  - [Postman API Testing](#)
  - [Rest Assured Guide](#)
- 

## **Week 6: Advanced Scanning & Enumeration**

#### **Goals:**

- ✓ Learn Nikto, Gobuster, Dirb for scanning
- ✓ Perform directory brute-forcing
- ✓ Enumerate services and open ports

#### **Hands-on Tasks:**

- ✓ Scan a target website using Nikto (`nikto -h <target>`)
- ✓ Find hidden directories using Gobuster (`gobuster dir -u <URL> -w <wordlist>`)

#### **Learning Resources:**

- Nikto Scanner Guide
  - [Gobuster Tool](#)
- 

## **Week 7: Exploitation with Metasploit**

#### **Goals:**

- ✓ Learn Metasploit for exploiting vulnerabilities
- ✓ Exploit a vulnerable machine
- ✓ Understand payloads and privilege escalation



#### **Hands-on Tasks:**

- ✓ Exploit a vulnerable VM (Metasploitable2)
- ✓ Create a reverse shell payload



#### **Learning Resources:**

- Metasploit Unleashed
  - TryHackMe - Metasploit
- 



## **Week 8: Wireless Security Testing**



#### **Goals:**

- ✓ Crack Wi-Fi passwords
- ✓ Use Aircrack-ng & Wifite for Wi-Fi hacking



#### **Hands-on Tasks:**

- ✓ Capture Wi-Fi handshakes using Airodump-ng
- ✓ Decrypt WPA2 passwords using Aircrack-ng



#### **Learning Resources:**

- Aircrack-ng Guide
- 



## **Week 9: Mobile App Security Testing**



#### **Goals:**

- ✓ Learn Android & iOS app security testing
- ✓ Reverse engineer APK files



#### **Hands-on Tasks:**

- ✓ Analyze an Android app using **Drozer**
- ✓ Bypass SSL pinning with **Frida**



#### **Learning Resources:**

- Drozer Tool Guide

- [Frida Mobile Security](#)
- 

## **Week 10: Cloud & Container Security**

### **Goals:**

- ✓ Test cloud security (AWS, Azure)
- ✓ Scan Docker images for vulnerabilities

### **Hands-on Tasks:**

- ✓ Scan a Docker container using Trivy
- ✓ Test an AWS S3 bucket for misconfigurations

### **Learning Resources:**

- [AWS Pentesting Guide](#)
  - Trivy for Container Security
- 

## **Week 11: Advanced Red Teaming & Privilege Escalation**

### **Goals:**

- ✓ Learn Windows & Linux Privilege Escalation
- ✓ Understand Active Directory attacks

### **Hands-on Tasks:**

- ✓ Use **WinPEAS** to find privilege escalation paths
- ✓ Exploit **Kerberoasting** for credential stealing

### **Learning Resources:**

- Windows PrivEsc Guide
  - TryHackMe - Active Directory
-

## **Week 12: Automating Security Testing in CI/CD**

### **Goals:**

- ✓ Integrate security tests in DevOps pipelines
- ✓ Use SonarQube & OWASP Dependency-Check




### **Hands-on Tasks:**

- ✓ Automate security scanning in a CI/CD pipeline
- ✓ Run SAST (Static Analysis) with SonarQube

### **Learning Resources:**

- [SonarQube Security Scanning](#)
  - OWASP Dependency-Check
- 

### **Final Steps:**

-  Take CTF challenges on **Hack The Box**, **TryHackMe**
-  Join **Bug Bounty Programs** (**HackerOne**, **Bugcrowd**)
-  Apply security automation in **Selenium**, **Cypress**

- 
-