1. SEED Labs - DNSSEC Lab

- **Objective**: Understand and configure DNSSEC to protect DNS queries.
- **Setup**:
    1. **Install Required Software**: Use `sudo apt-get install bind9utils` to install necessary tools on your host VM.
    2. **Generate Keys**: Use `dnssec-keygen` to create Zone Signing Key (ZSK) and Key Signing Key (KSK) for your domain.

```
dnssec-keygen -a RSASHA256 -b 1024 example.edu
dnssec-keygen -a RSASHA256 -b 2048 -f KSK example.edu
```

    3. **Sign Zone File**: Use `dnssec-signzone` to sign your domain's zone file.
    4. **Configure Nameserver**: Modify `named.conf.seedlabs` to use the signed zone file.
    5. **Testing**: Use `dig` commands to verify DNSSEC setup.

```
dig @10.9.0.65 example.edu DNSKEY +dnssec
```

- **Lab Environment**: Use Docker containers to simulate a miniature DNS infrastructure with a local DNS server, EDU server, and root server.

2. GNS3 Network Simulator

- **Objective**: Simulate network configurations and test firewall setups.
- **Setup**:
    1. **Install GNS3**: Download and install GNS3 on your computer.
    2. **Create a New Project**: Start a new project in GNS3.
    3. **Add Devices**: Drag and drop routers, switches, and firewalls into your project.
    4. **Configure Devices**: Use CLI to configure each device (e.g., setting up firewall rules).
    5. **Test Network**: Use tools like `ping` or `traceroute` to test connectivity and firewall effectiveness.

3. Blue Team Labs

- **Objective**: Practice defensive security techniques using IDS/IPS systems.
- **Setup**:
    1. **Access Blue Team Labs**: Register and access the Blue Team Labs platform.
    2. **Choose a Scenario**: Select a lab scenario focused on IDS/IPS.
    3. **Configure IDS/IPS**: Follow lab instructions to set up and configure IDS/IPS systems.
    4. **Analyse Traffic**: Use tools like Wireshark to analyse network traffic and identify threats.
    5. **Implement Mitigations**: Apply security measures based on your analysis.

4. VulnHub VMs

- **Objective**: Practice setting up honeypots and analysing attack patterns.

- **Setup**:
    1. **Download a VulnHub VM**: Choose a VM suitable for honeypot setup.
    2. **Set Up the VM**: Configure the VM in a virtualisation software like VirtualBox.
    3. **Configure Honeypot**: Follow lab instructions to set up a honeypot environment.
    4. **Monitor Attacks**: Use tools like Kibana or ELK Stack to monitor and analyse incoming attacks.
    5. **Analyse Logs**: Study logs to understand attack vectors and patterns.

5. OWASP Juice Shop

- **Objective**: Practice web application security testing.
- **Setup**:
    1. **Download OWASP Juice Shop**: Get the latest version of the Juice Shop application.
    2. **Set Up the App**: Deploy the app in a local environment or Docker container.
    3. **Identify Vulnerabilities**: Use tools like Burp Suite or ZAP to scan for vulnerabilities.
    4. **Exploit Vulnerabilities**: Follow lab instructions to exploit identified vulnerabilities.
    5. **Fix Vulnerabilities**: Apply patches or fixes to secure the application.

6. LabEx

- **Objective**: Practice network security and ethical hacking skills.
- **Setup**:
    1. **Access LabEx**: Register and access the LabEx platform.
    2. **Choose a Lab**: Select a lab scenario focused on network security or ethical hacking.
    3. **Follow Lab Instructions**: Complete tasks as guided by the lab scenario.
    4. **Practice Skills**: Use tools and techniques learned in the lab to enhance your skills.
    5. **Review Feedback**: Analyse feedback and improve your approach.