Create & Configure the Vulnerable WebApp VM

1. Prepare the VM

1. **New VM Settings**
   - **Name:** WebApp
   - **Type:** Linux → Version: Ubuntu (64-bit)
   - **Memory:** 2 GB RAM
   - **Disk:** 20 GB VDI, dynamically allocated
2. **Network Adapter**
   - **Adapter 1:** NAT Network → choose **Lab-DMZ**
   - **Adapter 2:** Internal adapter → choose **Lab-Internal**
3. **Attach Ubuntu ISO & Install**
   - Mount the latest Ubuntu Server ISO.
   - Install with defaults; create a non-root user (e.g., webadmin), enable OpenSSH.

2. Install LAMP & DVWA (Damn Vulnerable Web App)

Log into your Ubuntu VM as webadmin:

Terminal:

 # Elevate to root

sudo -i

 # Update and install LAMP stack with MariaDB

apt update && apt upgrade -y

apt install -y apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php

 # Secure MariaDB

mariadb-secure-installation

 # Start MariaDB server

sudo service mariadb start or sudo systemctl start mariadb

 # Create DVWA database and user

```
mysql -u root -p <<EOF
CREATE DATABASE dvwa;
GRANT ALL ON dvwa.* TO 'dvwauser'@'localhost' IDENTIFIED BY 'dvwapass';
FLUSH PRIVILEGES;
EOF
```

 # Download and deploy DVWA

```
cd /var/www/html
rm index.html
git clone https://github.com/digininja/DVWA.git
mv DVWA/* .
```

 # Configure DVWA

```
cp config/config.inc.php.dist config/config.inc.php
sed -i "s/$_DVWA[ 'db_user' ] = 'root';/$_DVWA[ 'db_user' ] = 'dvwauser';/; \
    s/$_DVWA[ 'db_password' ] = 'p@ssw0rd';/$_DVWA[ 'db_password' ] = 'dvwapass';/" \
  config/config.inc.php
```

 # Set permissions

```
chown -R www-data:www-data /var/www/html
chmod -R 755 /var/www/html
```

 # Enable Apache mods and restart

a2enmod rewrite

systemctl restart apache2

3. Configure DVWA

1. In **WebApp**'s Apache config (e.g., /etc/apache2/sites-available/000-default.conf), ensure:

<Directory /var/www/html>

AllowOverride All

</Directory>

2. Reload Apache:

Terminal:

systemctl reload apache2

3. **Access DVWA** from your host:

Terminal:

ip a

- In a browser on your Kali or host, navigate to http://<WebApp-IP>/setup.php
- Click **Create / Reset Database**.
- Login at http://<WebApp-IP>/login.php with credentials:
  - User: **admin**
  - Password: **password**

---

4. Test the Setup

- Verify you can log in to DVWA.
- Browse to **DVWA Security** and set it to **low** for initial testing.
- From Kali, try basic recon:

Terminal

nmap -sV <WebApp-IP>

curl http://<WebApp-IP>/login.php

🎉 **Complete!** You now have:

1. **Attacker VM** (Kali)
2. **DC1** (Windows Server, AD DS & DNS)
3. **Win10** (domain-joined)
4. **FileSrv** (SMB share)
5. **WebApp** (vulnerable DVWA in DMZ)