Denial of Service Practical – Slowloris Attack on DVWA (Metasploitable 2)

Aim of the Practical

To perform a Slowloris Denial of Service attack on DVWA hosted in Metasploitable 2 and observe the impact on website network stability and availability.

Description of the Practical

In this practical, a Slowloris attack is executed against the DVWA web application running on Metasploitable 2.
Slowloris is an application-layer DoS attack that opens multiple HTTP connections to the web server and keeps them half-open by sending incomplete HTTP requests. This exhausts the server's connection pool, making the website slow or unresponsive for legitimate users.

⚔️ Type of Attack Performed

- **Attack Name:** Slowloris
- **Category:** Denial of Service (DoS)
- **Attack Layer:** Application Layer (Layer 7)
- Target Application: DVWA
- **Tool Used:** Slowloris (Python-based)

🧪 Lab Setup

- **Attacker Machine**: Parrot Security OS
- **Victim Machine:** Metasploitable 2
- **Target Application:** DVWA

Step-by-Step Procedure

Step 1: Start Metasploitable 2

- Power on **Metasploitable 2**
- Login to the system
- Ensure the machine is running properly

Step 2: Open Browser in Parrot OS

- Start **Parrot Security OS**
- Open the browser
- Enter the following URL:

http://<target IP>

Step 3: Navigate to DVWA

- From the Metasploitable web page, click on **DVWA**
- DVWA login page will open

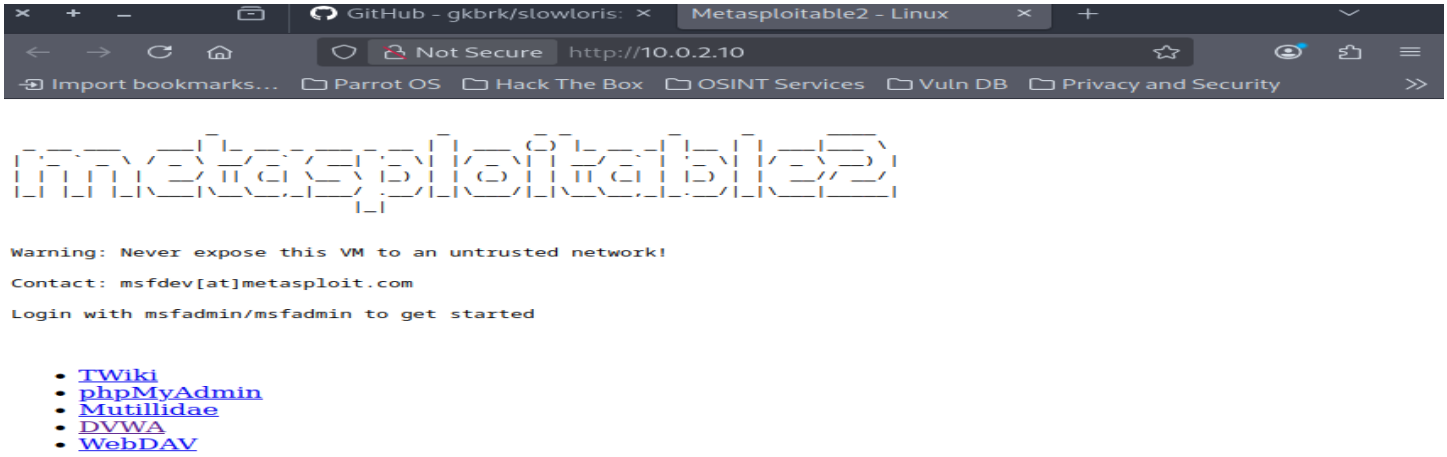
Step 4: Login to DVWA

Use the default credentials:

Username: admin

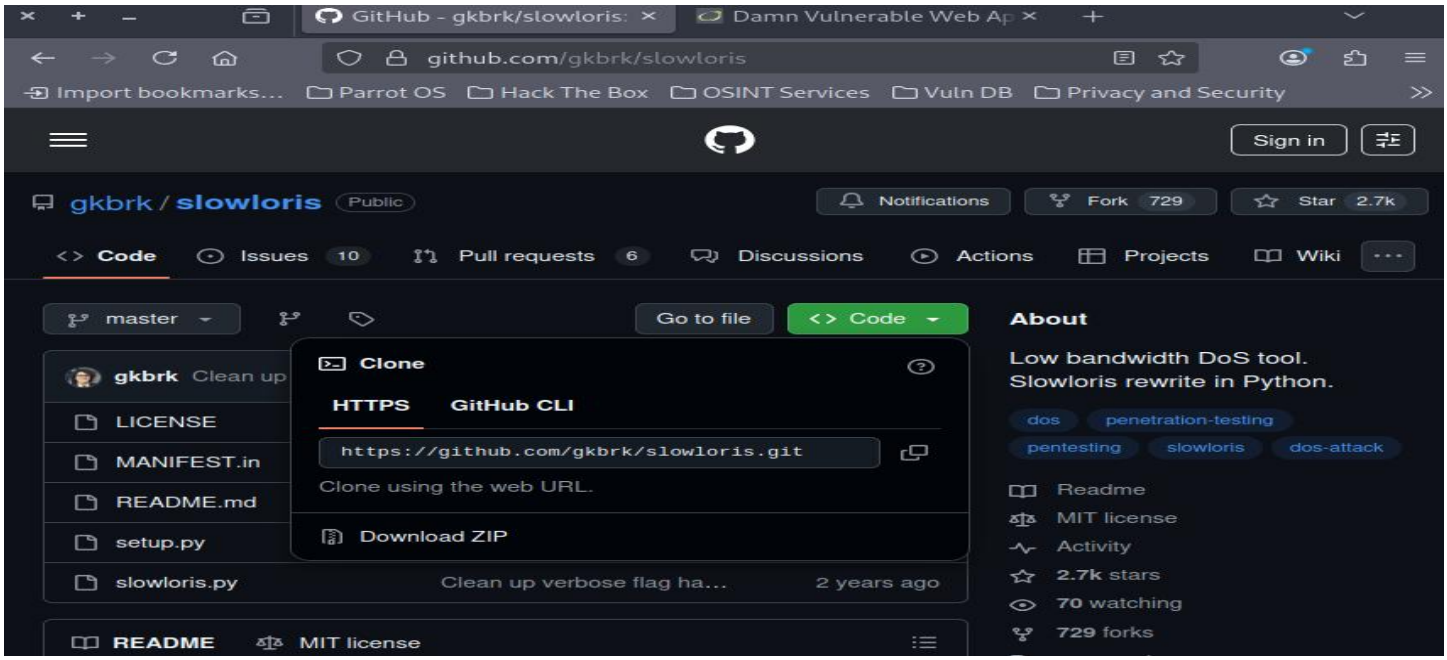
Password: password

- Login successfully
- Keep the DVWA page open



Step 5: Search Slowloris on GitHub

- Open a new tab
- Search for **Slowloris GitHub**
- Select a trusted Slowloris repository
- Copy the **repository URL**



Step 6: Clone Slowloris Repository

Open **Terminal** in Parrot OS and run:

git clone <slowloris_github_url>

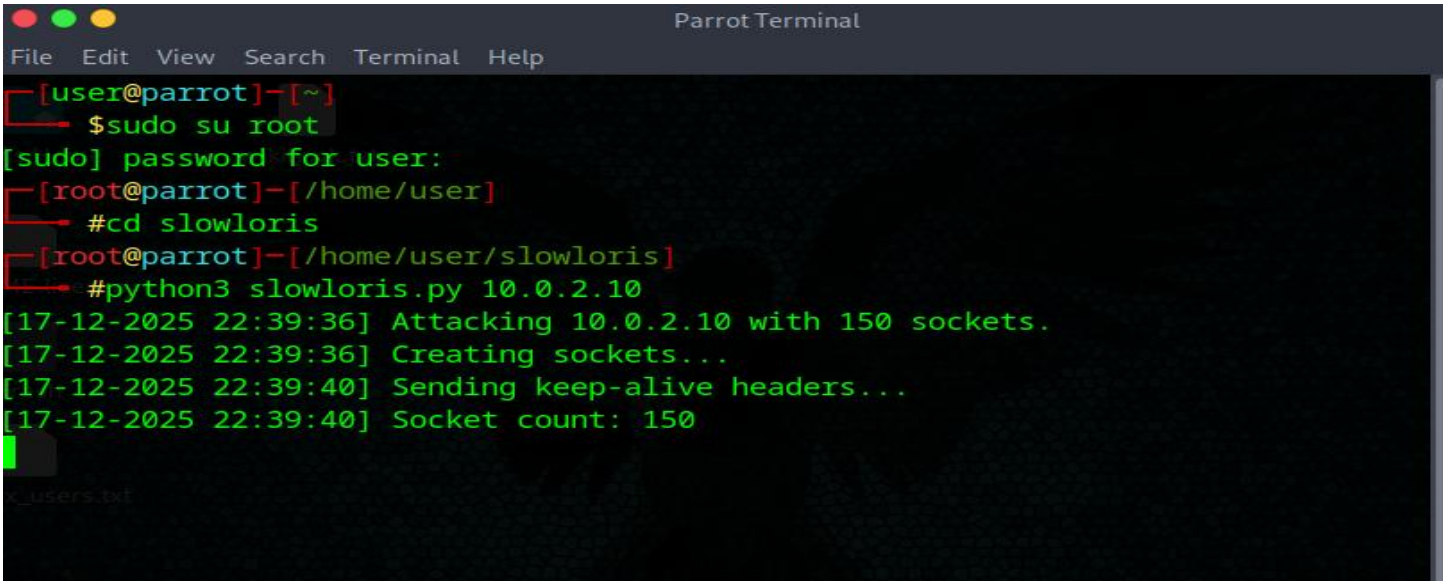
Step 7: Navigate to Slowloris Directory

cd slowloris

Step 8: Execute Slowloris Attack

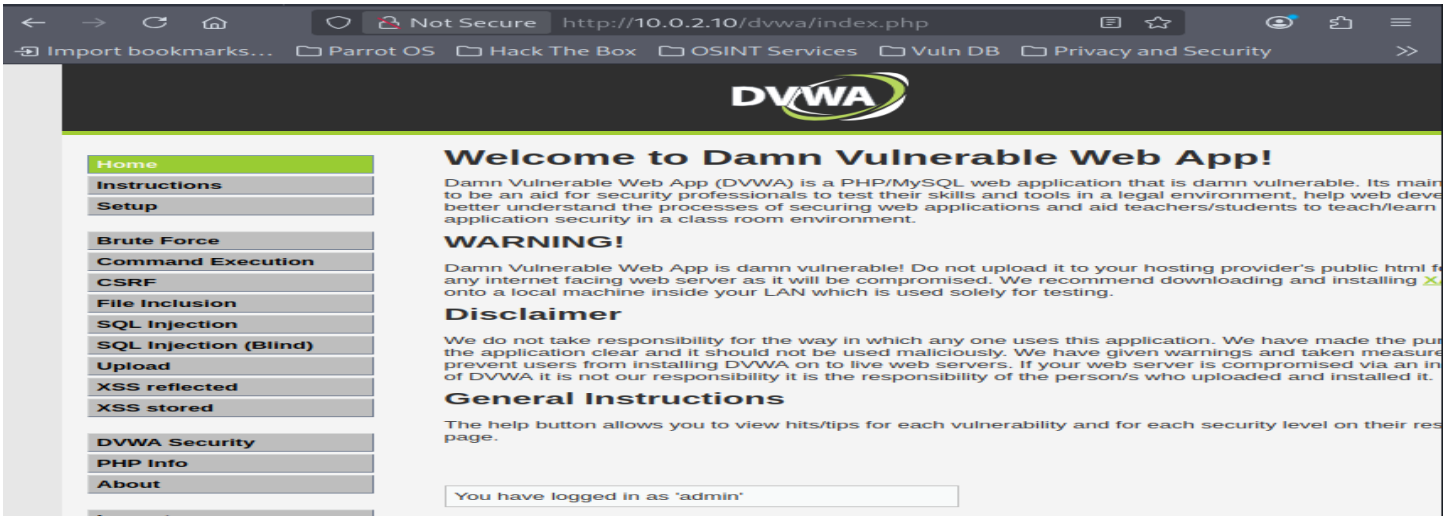
Run the following command:

python3 slowloris.py target IP



Step 9: Observe Website Behavior

- Go back to the DVWA webpage
- Refresh the page
- Try navigating to another DVWA page
- The website loads **very slowly or becomes unstable**
- Network delay is clearly visible



📊 Observation

- DVWA pages take longer to load
- Website becomes unstable when switching pages
- Apache server connections are exhausted
- Attack uses **low bandwidth but high impact**

✅ Result

The **Slowloris DoS attack** was successfully performed on **DVWA running in Metasploitable 2**.
The attack demonstrated how keeping multiple HTTP connections half-open can disrupt the availability of a vulnerable web application.

🛡️ Mitigation Techniques

- Enable mod_reqtimeout in Apache
- Configure Web Application Firewall (WAF)
- Limit maximum concurrent connections
- Apply server hardening and patches

⚠️ Ethical Disclaimer

This practical was conducted **only in a controlled virtual lab environment** using intentionally vulnerable systems for educational purposes.