# 🛡️ DoS in Python: Simulate the Storm, Build the Shield

***Unleash the flood, then hold the line — explore both sides of cybersecurity through live Python coding.***

## Facilitators:

- Shuvalaxmi Dass, PhD. <shuvalaxmi.dass@louisiana.edu>
- Moitrayee Chatterjee, PhD. <mchatterjee@njcu.edu>
- Rishika Ak. <rishika51896@gmail.com>

---

## Workshop Description:

Denial-of-Service (DoS) attacks are among the most disruptive and fast-growing threats in cyberspace today. As of 2024, Cloudflare reported an average of 2,200 DDoS attacks per hour, with global daily incidents reaching 23,000—a staggering 81.7% increase from 2023.

Understanding how to simulate, detect, and mitigate these attacks is a crucial skill for cybersecurity professionals. This workshop offers a **hands-on introduction to both offensive and defensive cybersecurity using Python**, empowering participants to simulate DoS attacks and write code to defend against them — all in a **safe, ethical, and isolated lab environment**.

Whether you're an early-career security enthusiast, educator, or researcher, this session is designed to give you real-world experience with coding tools and attack-response workflows that are foundational to modern cybersecurity.

> ⚠️ **Note**: All activities are for educational purposes only and will take place in isolated environments with ethical safeguards.

---

## Workshop Duration: 60 minutes

### 1. Introduction & Threat Landscape (10 min)

- Welcome and meet the facilitators
- Overview of:
  - How DDoS attacks work (layers, vectors, real-world examples)
  - The importance of Python in cybersecurity
  - Ethical hacking principles
- Brief look at Python libraries used: `requests`, `socket`, `Flask`, `Flask-Limiter`, `re`, `matplotlib`

🛠️ *Goal: Set the stage by contextualizing the problem and introducing the tools.*

---

**2. Offensive Coding Session – Simulating DDoS Attacks (15 min)**

Participants will write Python scripts to simulate two types of attacks in a lab environment:

- **HTTP Flood**: Sending large volumes of GET requests to a target server
- **SYN Flood (Conceptual)**: Overview of TCP SYN flood and scripting basics using `socket`

We'll use tools like `ngrok` or similar to expose Flask servers for testing.

🛠️ *Goal: Understand attacker behavior by writing simple attack scripts. This demystifies offensive tactics and lays a foundation for defense.*

---

**3. Defensive Coding Session – Detecting and Mitigating Attacks (15 min)**

Participants will switch roles and act as defenders by:

- **Implementing rate limiting** using `Flask-Limiter`
- **Blocking abusive IPs** via basic Python logic
- **Parsing logs** using regular expressions to detect anomalies

🛠️ *Goal: Equip participants to defend web applications using Python-powered detection and throttling methods.*

---

**4. Attack-Defense Observation Tasks (10 min)**

Participants will analyze logs and server behavior in real-time:

- Monitor server logs for suspicious patterns (e.g., repetitive IPs, high request volume)
- Track Flask server response codes (especially 429 - Too Many Requests)
- Visualize rate limiting effects using `matplotlib`
- Modify `default_limits` and see how performance changes

🛠️ *Goal: Practice situational awareness — a critical skill in cyber defense — through interactive feedback and visual cues.*

---

**5. Wrap-Up, Q&A & Career Paths (10 min)**

- Troubleshooting and sharing code
- Summary of offensive and defensive strategies
- Introduce real-world roles where these skills are applied:
    - Penetration Tester / Red Team
    - Security Analyst / Blue Team
    - Security Automation Engineer
- Share GitHub repo and further learning resources

🛠️ *Goal: Reflect, ask questions, and explore next steps in the field.*

---

## Prerequisites:

- Basic Python programming knowledge (variables, loops, functions)
- BYOD (Bring Your Own Device) with access to browser-based Python environments such as Google Colab.

---

## Target Audience:

- Early to mid-career professionals in cybersecurity
- Educators and students seeking practical experience
- Industry participants exploring Python’s role in security

---

## Key Takeaways:

- Learn how basic DDoS attacks are scripted and simulated
- Understand the logic and implementation of Python-based defenses
- Gain hands-on experience with attack-response workflows
- Get inspired to explore offensive or defensive career paths in cybersecurity

---

## Knowledge Sharing:

All code, slides, and documentation will be shared via GitHub and/or Google Drive. Participants will also receive links to further labs, videos, and certifications.

---

## Why This Workshop Matters:

Cybersecurity remains one of the most in-demand yet underrepresented fields in tech. With over 3.5 million jobs projected by 2025, accessible workshops like this are critical to engaging diverse talent.

This session helps close that gap by:

- Making advanced security concepts approachable through Python
- Providing guided, hands-on labs led by women in cybersecurity
- Encouraging underrepresented groups to enter and thrive in security careers

---

GitHub Repository:

https://github.com/moicha/DoS-in-Python-Simulate-the-Storm-Build-the-Shield.git

---

## 📚 References

[1] https://cybersecurityventures.com/jobs/<br>
[2] https://www.cyberseek.org/<br>
[3] https://myturn.careers/blog/future-of-cybersecurity-job-market/<br>
[4] https://www.zippia.com/cyber-security-specialist-jobs/demographics/<br>
[5]https://www.careerera.com/blog/what-is-the-percentage-of-women-in-cybersecurity<br>
[6] Why are DDoS attacks so hard to stop? | PC Gamer