DOS Detection

Packet Capture:

- Use `tcpdump` to capture live traffic:

```
sudo tcpdump -i eth0 -w traffic.pcap
```

DOS detection logic:

- Use `scapy` in Python to read and analyze packets:

```
from scapy.all import rdpcap
packets = rdpcap('traffic.pcap')
```

- Use the same logic as previously mentioned, but ensure that you have installed all the necessary dependencies for **Scapy** to work properly on Windows. Here's a sample Python script:

```
from scapy.all import sniff, IP

def detect_dos(pkt):
    if pkt.haslayer(IP):
        src_ip = pkt[IP].src
        # Implement rate limiting or pattern detection logic
here
        if is_abnormal_traffic(src_ip):
            alert("Potential DOS attack from IP: " + src_ip)

sniff(prn=detect_dos, store=0)
```

Simulate DOS Attacks:

- Use LOIC or other stress testing tools available for Windows to simulate DOS attacks.

- Use tools like `hping3` to generate DOS traffic for testing.

Validation:

- Test your detection system against the simulated attacks and ensure it is working correctly.