Step-by-Step Procedure: Intrusion Detection System using Packet Analysis

1. Set Up Your Host Machine (Windows)

- Install Python from https://www.python.org/downloads/ and add it to PATH.
- Open CMD or PowerShell and run: pip install scapy
- Download and install Npcap from https://nmap.org/npcap/
- During install, check 'Install Npcap in WinPcap API-compatible mode' and 'Support raw 802.11 traffic'.

2. Create Virtual Machine (Attacker)

- Download Kali Linux ISO: https://www.kali.org/get-kali/
- Create VM in VirtualBox with Bridged Adapter selected for networking.

3. Verify Network Connection

- On Host: Run ipconfig and note IPv4 (e.g., 192.168.0.20).
- On Kali: Run ip a and verify similar subnet (e.g., 192.168.0.21).
- From Kali: ping 192.168.0.20. If it fails, adjust firewall settings.

4. Create the IDS Python Script (main.py)

- Use the following code:

```
- from scapy.all import sniff, IP, TCP
-
- packet_count = {}
- THRESHOLD = 100
-
- def detect_syn_flood(pkt):
-     if IP in pkt and TCP in pkt:
-         if pkt[TCP].flags == 'S':
-             src_ip = pkt[IP].src
-             packet_count[src_ip] = packet_count.get(src_ip, 0) + 1
-             print(f"[LOG] SYN from {src_ip}, count: {packet_count[src_ip]}")
-             if packet_count[src_ip] > THRESHOLD:
-                 print(f"[ALERT] Possible SYN Flood from {src_ip}!")
-
```

- sniff(filter="tcp", prn=detect_syn_flood, store=0)

5. Run the IDS on Windows Host

- Open CMD or PowerShell as Administrator.
- Run: python main.py

6. Simulate Attack from Kali VM

- Install hping3: sudo apt update && sudo apt install hping3
- Start SYN flood: sudo hping3 -S -p 80 --flood 192.168.0.20

7. Observe Logs on Host

- Expected Output:
- [LOG] SYN from 192.168.0.21, count: 1
- [LOG] SYN from 192.168.0.21, count: 101
- [ALERT] Possible SYN Flood from 192.168.0.21!

8. Analyze the Behavior

- Stop both scripts with Ctrl+C.
- Explain how detection worked, threshold used, and number of packets.