Python IDS Project – Windows 10

Core Libraries

- scapy (packet sniffing, needs Npcap, run as Admin)
- psutil (monitor processes & connections)
- pywin32 (read Windows Event Log for brute-force)
- watchdog (monitor firewall logs)
- Optional: pydivert (fast packet capture), pyshark (deep parsing)

Detection Methods

1. DDoS
- scapy/pydivert: count packets/sec per IP.
- psutil: watch surge in simultaneous connections.
- Firewall log: monitor with watchdog.

2. Nmap Scan
- scapy/pydivert: detect many SYNs to many ports.
- psutil: short-lived connections to closed ports.
- Rule: ≥20 ports in 5–10s → likely scan.

3. Brute Force (RDP/SMB)
- pywin32: read Security log.
- Event ID 4625: Failed logon.
- Event ID 4624: Successful logon.
- Threshold: ≥5 failures from same IP in 2 min.

Windows Setup Tips

- Install Npcap (WinPcap mode) for scapy.
- Run sniffer as Admin.
- Enable Security auditing for logon events.
- Optional: enable firewall logging for watchdog.