IPS Project - Detailed Team Roles Guide

1. Networking Team
- Build the virtual environment (Ubuntu victim, Kali attacker, Security Onion monitor).
- Connect all VMs inside the same internal network.
- Capture traffic (normal + attack) and export as PCAP files.
- Deliver PCAP files to AI Team.

2. AI Team
- Convert PCAP to structured data (CSV/JSON).
- Train a Machine Learning model (e.g., Random Forest).
- Export trained model as .pkl file.
- Deliver model + preprocessing scripts to Backend Team.

3. Backend Team (.NET Core)
- Develop ASP.NET Core Web API.
- Integrate AI model into API.
- Create endpoint /detect for attack detection.
- Deliver working API to Frontend + DevOps.

4. Frontend Team
- Build Dashboard (React/Vue.js).
- Display detected attacks and alerts in real-time.
- Integrate with Backend API.
- Deliver frontend code to DevOps.

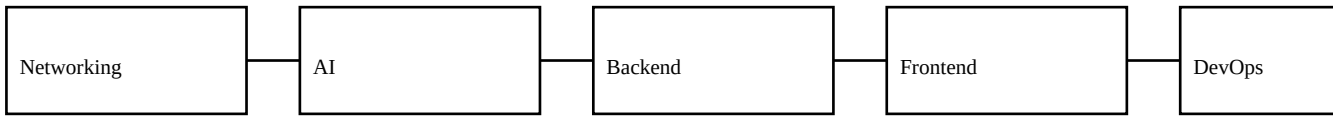
5. DevOps Team
- Containerize all components (Backend, Frontend, etc.).
- Deploy on AWS/Azure using Docker and GitHub Actions.
- Ensure CI/CD pipeline is working.
- Deliver final running system link to Pentest team.

6. Penetration Testing Team
- Attack the deployed system using various tools (Nmap, SQLmap, Flood attacks).
- Write report about weaknesses and suggestions.
- Deliver report to Incident Response Team.

7. Incident Response Team
- Monitor alerts and verify real vs false alarms.
- Collect evidence of incidents.
- Write detailed incident reports.
- Deliver reports to management.

Flow: Networking → AI → Backend → Frontend → DevOps → Pentesting → Incident Response

Team Integration Diagram


Networking
AI
Backend
Frontend
DevOps