SmartShield — Personal Firewall (Monitor-only)

Author: Avinash Patwal

Abstract
SmartShield is a lightweight personal firewall monitor that captures live network metadata, applies configurable rule checks (IP, port, protocol), and displays flagged events in a modern dark-themed GUI. The project focuses on packet capture using Scapy, rule-based detection, secure logging, and an interactive rule manager — all presented in a professional interface suitable for internship submission and interviews.

Introduction
Personal systems benefit from an additional layer of visibility into network activity. SmartShield provides real-time monitoring and a simple rule engine to help users identify suspicious traffic. The monitor-only design ensures safety during testing and evaluation without modifying system firewall rules.

Tools & Technologies
- Python 3.8+
- Scapy (packet capture)
- Tkinter (GUI)
- JSON for configuration
- Flat-file logging (smartshield_monitor.log)

Implementation Overview
1. **Packet capture:** Scapy's `sniff()` function runs in a background thread, summarizing each packet (timestamp, src, dst, proto, ports).
2. **Rule engine:** Rules are stored in `rules.json` (block_ips, block_ports, block_protocols). The GUI flags packets that match these rules.
3. **GUI & UX:** Modern dark-themed Tkinter UI with a live Treeview showing packets, an event box with recent flagged events, and a Rule Manager to edit rules at runtime.
4. **Logging:** Each observed packet is appended to `smartshield_monitor.log` with a standardized format for audit.

Testing & Sample Results
Environment: Ubuntu 22.04 (monitor-only), Python 3.10
Sample actions & results (excerpt):
```
2025-10-17T14:12:05Z | ICMP | 192.0.2.123 -> 198.51.100.45 | type=8 code=0  [FLAGGED] IP match
2025-10-17T14:12:08Z | TCP  | 10.0.0.5 -> 93.184.216.34 | sport=49212 dport=80  [OK]
2025-10-17T14:12:11Z | TCP  | 10.0.0.5 -> 203.0.113.7 | sport=50123 dport=23  [FLAGGED] Port 23
```
These sample results demonstrate that SmartShield correctly flags traffic matching configured rules and persists logs for auditing.

Limitations & Future Work
- Currently uses exact matches for IPs and ports. Future versions can add CIDR support, rate-limiting, and ML-based anomaly detection.
- Cross-platform enforcement (Windows/macOS) would require platform-specific APIs.
- A web-based dashboard (Flask) could complement the Tkinter UI for remote monitoring.

Conclusion

SmartShield is a compact, professional monitor-only personal firewall suitable for internships and demonstrations. It balances safety and functionality, offering clear paths for extension into enforcement, analytics, and richer UIs.

End of Report