

Blue Team
ivan notes 2022

1. Fundamentals



2. Threat Modeling



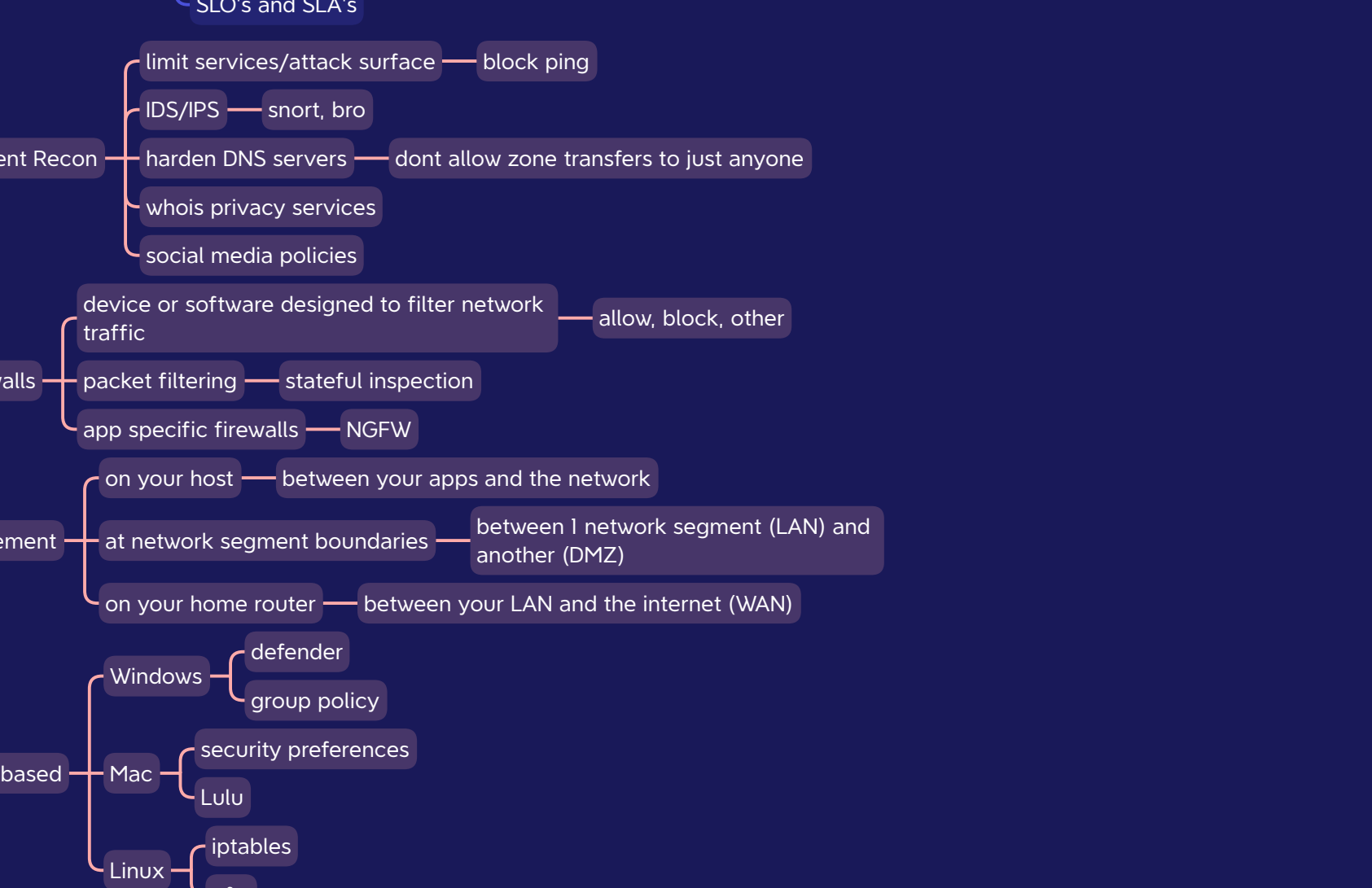
3. Asset Mgmt



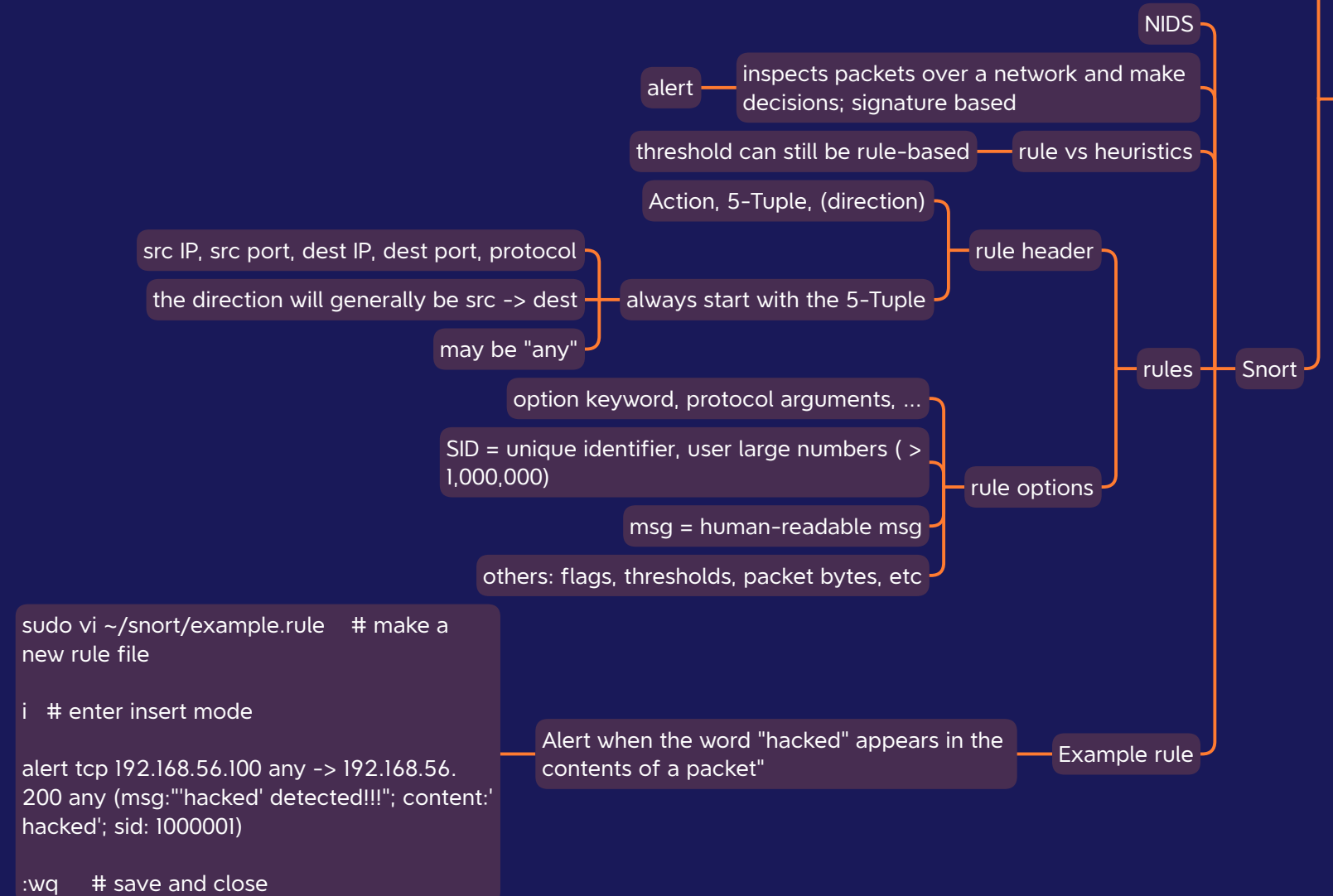
4. Vulnerability Mgmt



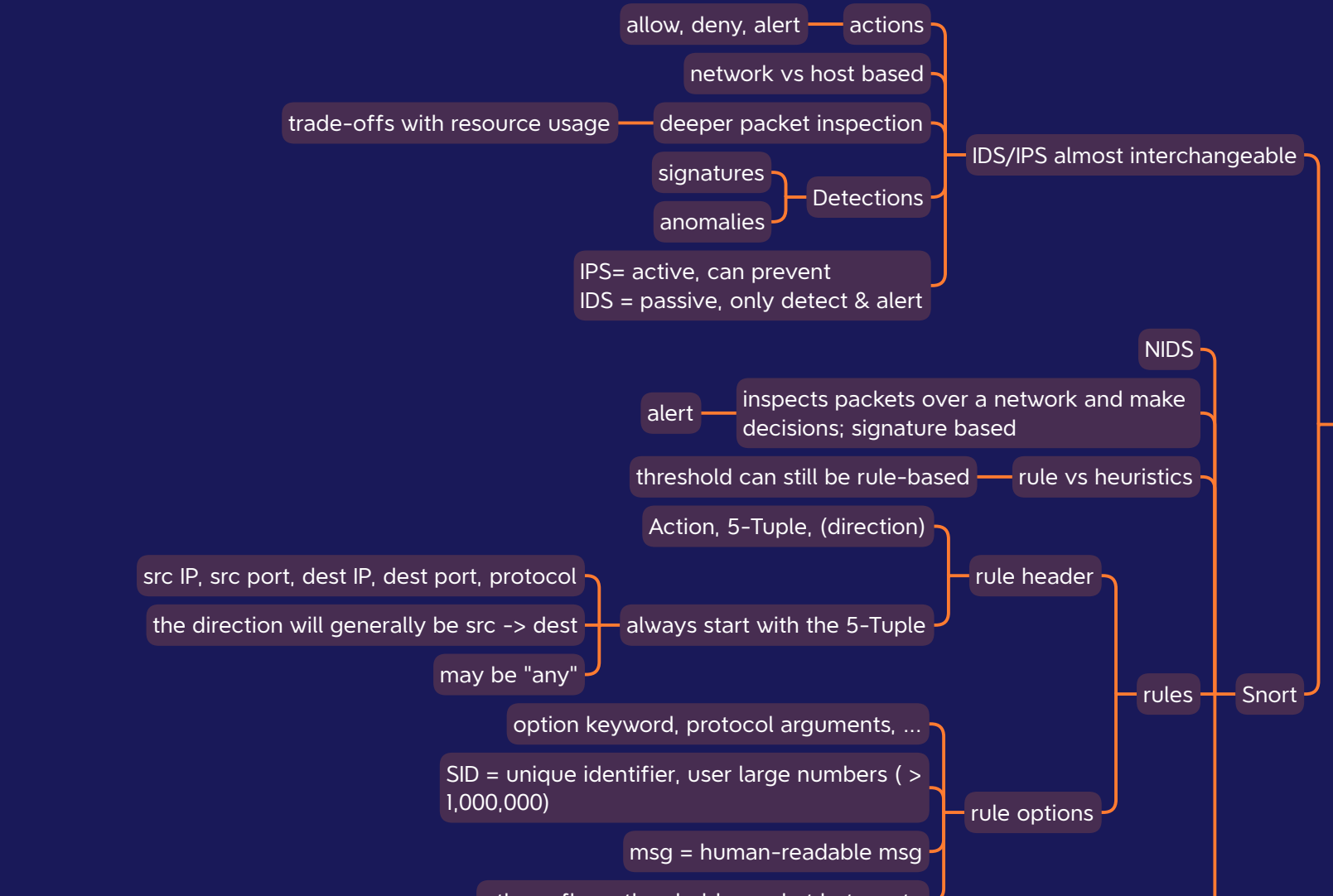
5. Firewalls



6. IDS/IPS



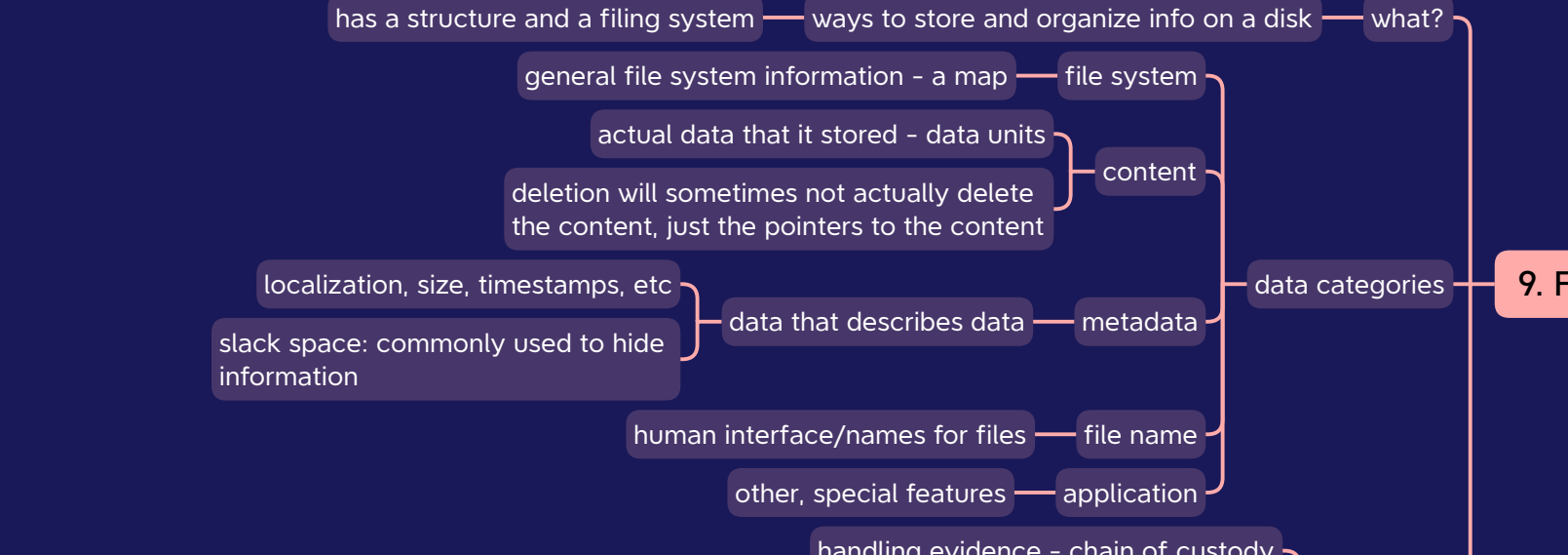
7. Defense in Depth



8. Logs



9. File Systems



10. Incident Response

