# Security Audit & Incident Response Using NIST Framework

Performed a comprehensive security audit and applied the NIST Cybersecurity Framework to respond to a real-world style incident. The work included evaluating existing security controls and compliance practices, identifying risks, and developing a mitigation plan for a DDoS attack scenario.

**Tools:** None specified (framework and documentation based)
**Skills:** Security auditing, compliance assessment, NIST CSF application, incident response planning, DDoS mitigation strategies
**Frameworks:** NIST Cybersecurity Framework, PCI DSS, GDPR, SOC 2

## Part 1: Security Audit & Compliance Assessment

- Conducted a controls assessment covering least privilege, firewalls, IDS, backups, encryption, password management, and disaster recovery.
- Evaluated compliance with PCI DSS, GDPR, and SOC 2 requirements.
- Identified missing controls such as MFA, RBAC enforcement, and incident response planning.
- Recommended improvements:
  1. Enforce Role-Based Access Control (RBAC) for sensitive data
  2. Implement Multi-Factor Authentication (MFA)
  3. Schedule regular compliance audits
  4. Conduct cybersecurity awareness training
  5. Maintain and test incident response plans

## Part 2: Applying NIST CSF to a DDoS Attack

**Scenario Summary:** A Distributed Denial of Service (DDoS) attack using ICMP flood traffic disabled internal network services for two hours due to an unconfigured firewall.

| | |
|---|---|
| Identify | Determined vulnerability from missing firewall configuration. |
| Protect | Implemented ICMP traffic limits, IP verification, IDS/IPS deployment, and firewall reviews. |
| Detect | Deployed network monitoring tools and set traffic threshold alerts. |
| Respond | Blocked ICMP packets, shut down non-critical services, restored critical operations first. |
| Recover | Restored systems, verified performance, conducted root cause analysis, and scheduled firewall audits. |

## Outcome

Produced a comprehensive security posture report that aligns with industry compliance standards. Strengthened the organization’s defensive capabilities against DDoS attacks. Demonstrated ability to integrate auditing and incident response frameworks into actionable security improvements.