Cybersecurity Capstone Project: DDoS Attack Incident Response Playbook

1. Aim and Objective

The aim of this project is to develop a detailed Incident Response (IR) playbook for Distributed Denial of Service (DDoS) attacks. The objective is to equip the organization with a structured process to quickly detect, mitigate, and recover from DDoS attacks, ensuring service availability and minimizing downtime while protecting infrastructure from sustained disruptions.

2. Methodology

Concept of Project

DDoS attacks overwhelm network resources by flooding servers with excessive traffic, causing service outages or degraded performance. This playbook provides a clear, actionable response framework that leverages advanced detection technologies and mitigation strategies, including traffic filtering and scrubbing. Emphasis is placed on timely detection, rapid response, clear role definitions, and communication plans to coordinate internal teams and external service providers effectively.

Tools Used

1. **DDoS Mitigation Services:** Cloudflare, Akamai Kona Site Defender, AWS Shield, or Radware DefensePro for real-time traffic scrubbing

2. Network Monitoring & SIEM: SolarWinds, Nagios, Splunk, or Microsoft Sentinel to detect traffic anomalies and generate alerts

3. Firewall & Load Balancers: Cisco ASA, Palo Alto Networks, F5 BIG-IP for traffic filtering and rate limiting

4. Incident Management Platforms: Jira Service Management, ServiceNow for tracking response tasks

5. Communication Tools: Microsoft Teams, Slack for rapid internal coordination; secure email for external communication with ISPs or law enforcement

3. Incident Playbooks

DDoS Attack Incident Response Playbook

Incident Identification: Triggers and Indicators

– Sudden spike in inbound traffic volume, especially from multiple IP sources (botnets)

– Network monitoring alerts showing abnormal bandwidth consumption or packet floods

– Service degradation or unavailability reported by users or automated uptime monitors

– SIEM alerts correlated with unusual traffic patterns, high SYN/UDP/ICMP requests

– Network devices (firewalls/load balancers) logging excessive dropped packets or error rates

Incident Response Phases

1. Detection:

– Real-time traffic monitoring and alerting via SIEM and monitoring tools

– Expected detection time: within 5 minutes of abnormal traffic onset

2. Containment:

– Activate DDoS mitigation services (Cloudflare, AWS Shield) to filter and scrub traffic within 10 minutes of detection

– Implement rate limiting and blackhole routing on firewalls/load balancers within 15 minutes

– Coordinate with ISP or upstream providers to block malicious traffic at the edge within 30 minutes

3. Eradication:

– Sustain filtering rules and adjust mitigation thresholds to block attack vectors while maintaining legitimate traffic flow over several hours as needed

– Monitor for attack subsidence; adjust firewall rules to prevent recurrence

Recovery:

– Gradual removal of filtering measures once attack traffic subsides to restore full service performance within 2 hours

– Conduct network health checks and validate service functionality post–attack

– Review logs for signs of follow–up attacks for at least 48 hours post–event

Roles and Responsibilities

– Incident Commander: Oversees the entire response, liaises with external partners including ISPs and mitigation vendors

– Network Security Engineer: Manages firewall/load balancer configurations, activates mitigation services, monitors traffic flow

– SOC Analyst: Monitors SIEM alerts, verifies attack indicators, and updates incident status

- IT Operations: Ensures service uptime where possible, communicates with affected user groups
- Communications Officer: Coordinates internal updates, external notifications, and manages communication with stakeholders and regulators

Communication Strategy

Internal:

- Immediate alert to SOC, network, and management teams within 5 minutes of detection
- Status updates every 30 minutes during the active attack phase
- Post-incident briefing within 24 hours of attack resolution

External:

- Notify upstream ISP and DDoS mitigation service providers immediately upon detection
- Regulatory notification if service outage exceeds thresholds (e.g., 1 hour downtime for critical services)
- Customer communication through official channels within 1 hour of confirmed service disruption

Metrics

Metric	**Target Time/Value**	**Tool for Measurement**
Time to Detect	⩽ 5 minutes	SIEM (Splunk, Microsoft Sentinel) alerts
Time to Activate Mitigation	⩽ 10 minutes after detection	DDoS mitigation service logs (Cloudflare, AWS Shield)

Time to Contain Traffic	≤ 15 minutes post-detection	Firewall/load balancer logs
Duration of Attack	Monitored, varies; aim to minimize	Network monitoring tools
Service Downtime	≤ 1 hour for critical services	Uptime monitoring (Nagios, SolarWinds)
User Impact	Minimized user complaints, tracked	Helpdesk ticketing system

4. Presentation/Report

Design Choices Explanation

The playbook focuses on ultra-rapid detection and mitigation due to the immediate and high-impact nature of DDoS attacks. Using cloud-based DDoS mitigation services allows for scalable, real-time traffic filtering beyond the organization's on-premise capabilities. Coordination with ISPs ensures malicious traffic is blocked upstream, reducing load on internal infrastructure. Clearly defined roles enable smooth task allocation during high-pressure events, while regular communication updates maintain situational awareness among stakeholders. Metrics prioritize minimizing downtime and ensuring quick activation of mitigation tools.

Expected Benefits

- Minimized service disruption and improved availability during DDoS attacks
- Clear, coordinated response reduces confusion and speeds mitigation
- Leveraging cloud mitigation services enhances defense capability beyond local resources
- Timely communication fosters transparency with users and regulators
- Metrics enable performance evaluation and continual improvement

5. Post-Incident Review Template

Section: Details to Capture

Incident Description: Summary of DDoS attack, vectors used, duration, and affected services

Detection: Detection timeline, tools involved, alerts generated

Response Actions: Timeline of mitigation activations, firewall changes, ISP coordination

Roles & Communication: Effectiveness of team roles and communication flow

Challenges Faced: Technical or coordination challenges during mitigation

Metrics Results: Actual vs target detection and containment times, service downtime

Lessons Learned: Identification of vulnerabilities in infrastructure or response process

Recommendations: Suggestions for improving detection capabilities, mitigation contracts, or communication protocols

Follow–up Actions: Assigned owners and deadlines for follow–up measures and audits

6. Conclusion

This DDoS Attack Incident Response Playbook equips the organization with a rapid, coordinated response strategy that leverages advanced mitigation technologies and strong communication protocols. By emphasizing quick detection and mitigation activation within minutes, the playbook aims to sustain service availability and minimize the operational impact of DDoS attacks. Post–incident reviews and measurable metrics ensure ongoing improvements to the organization’s DDoS resilience.

7. Reference

NIST SP 800–61 Revision 2: Computer Security Incident Handling Guide

SANS Institute DDoS Mitigation Resources

Cloudflare DDoS Protection Documentation

Akamai Kona Site Defender User Guide

AWS Shield Advanced Whitepapers

Cisco ASA and Palo Alto Networks Firewall Configuration Guides

SolarWinds Network Performance Monitor Documentation