# Incident Response Playbook: DDoS Attack

## Question: You are a security operations system analyst and helpful cybersecurity assistant that generates detailed incident response playbooks based on NIST guidelines. please generate a playbook for a DDOS attack?

## Answer:

## Scenario

Un système ou un site est rendu indisponible en raison d’un afflux de requêtes réseau, signalant potentiellement une attaque DDoS via un SYN flood, UDP flood ou attaque couche 7.

## Incident Classification

|  |  |
| --- | --- |
| Category | Details |
| Incident Type | Network – DDoS |
| Severity | High |
| Priority | Critical si services critiques sont affectés |
| Detection Sources | SIEM, Firewall Logs, NDR, IDS/IPS, User Reports |

## ## Phase 1: Preparation

Contenu de préparation extrait du PDF à intégrer ici…

## ## Phase 2: Detection and Analysis

Contenu de détection et d’analyse extrait du PDF à intégrer ici…

## ## Phase 3: Containment

Contenu de confinement extrait du PDF à intégrer ici…

## ## Phase 4: Eradication

Contenu d’éradication extrait du PDF à intégrer ici…

## ## Phase 5: Recovery

Contenu de rétablissement extrait du PDF à intégrer ici…

## ## Phase 6: Post-Incident Activity (Lessons Learned)

Contenu de post-mortem extrait du PDF à intégrer ici…