# Incident Response Playbook: Denial-of-Service (DoS) 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 DOS attack?
* Answer:

## Scenario

Un pic soudain de trafic réseau ou une indisponibilité soudaine d’un service ou site web alerte les systèmes de détection (SIEM, IDS/IPS). Les utilisateurs signalent un ralentissement ou une impossibilité d'accès aux services. L’analyse révèle un flux anormal, possiblement causé par un SYN Flood, un UDP Flood, ou un HTTP GET/POST Flood.

## Incident Classification

|  |  |
| --- | --- |
| Category | Details |
| Incident Type | Network - Denial-of-Service (DoS) |
| Severity | High |
| Priority | Critical si services critiques sont touchés |
| Detection Sources | SIEM, IDS/IPS, NDR, Firewall logs, User Reports |

## Phase 1: Preparation

• Security Controls  
 - Déployer un Web Application Firewall (WAF) pour filtrer les requêtes malveillantes.  
 - Définir des politiques de limitation de débit sur les serveurs et APIs.  
 - Activer des services de protection DDoS (Cloudflare, AWS Shield, etc.).  
  
• Incident Response Setup  
 - Former une équipe de réponse DoS avec des rôles clairs.  
 - Maintenir les diagrammes réseau et inventaires d'actifs à jour.  
  
• User Awareness  
 - Former le personnel à reconnaître les signes d’une attaque DoS (ex. : indisponibilité soudaine d’un service).

## Phase 2: Detection and Analysis

• Identify Threat Indicators  
 - Réseau : pics de trafic entrants, répétition de requêtes sur un même endpoint, saturation de bande passante.  
 - Système : consommation CPU/mémoire anormale, délais/réponses prolongées.  
  
• Identify Risk Factors  
 - Communs : indisponibilité temporaire, pertes financières.  
 - Spécifiques : impact sur services clients, opportunité d’attaques secondaires.  
  
• Data Collection  
 - Logs : analyser les journaux de pare-feu, routeur et serveur.  
 - Trafic : utiliser Wireshark, SolarWinds ou équivalent pour analyser les paquets.  
  
• Categorise  
 - Vecteurs d’attaque : TCP SYN Flood, UDP Flood, HTTP GET/POST Flood  
  
• Is it an Advanced Attack?  
 - Indicateurs : attaque DDoS distribuée via botnets, spoofing IP, attaques couche 7 (Layer 7).  
  
• Triage  
 - Impact : identifier les services affectés, estimer la durée de coupure.  
 - Priorisation : critique si services clés impactés.  
  
• False Positive Check  
 - Comparer les schémas de trafic aux données historiques.

## Phase 3: Containment

• Contain the Threat  
 - Appliquer des règles de limitation de débit.  
 - Bloquer les adresses IP ou plages IP malveillantes.  
 - Rediriger le trafic via un service de mitigation DDoS.

## Phase 4: Eradication

• Eradicate Root Cause  
 - Corriger et renforcer les services vulnérables.  
 - Désactiver les services réseau inutilisés.  
  
• Validate  
 - S’assurer que le trafic légitime passe et que le trafic malveillant est bloqué.

## Phase 5: Recovery

• Restore Operations  
 - Lever progressivement les restrictions.  
 - Surveiller le trafic pour détecter toute récidive.  
  
• Post-Incident Recovery  
 - Informer les utilisateurs affectés des mesures prises.  
 - Réaliser une vérification complète de l’état des systèmes.

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

• Réaliser une analyse post-incident pour identifier les lacunes.  
• Mettre à jour les playbooks et renforcer les contrôles.  
• Effectuer des tests réguliers de simulation d’attaque DoS.