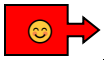
# You Shall Not Pass!



## DDoS (Distributed Denial of Service) Attack Response Plan

**The Facts Were These:** Custom cosplay costume designer Jan Van Gandalf's website becomes inaccessible due to a flood of malicious traffic.

*Below is a breakdown of each phase of the plan and a rough estimate of the timeline starting from the detection of the threat to the recovery stage.*

## Immediate Actions (0-15 minutes)

### Detection

Website becomes slow or inaccessible.
Network monitoring alerts for unusual traffic.
Customer complaints about service availability.
ISP notifications of traffic anomalies.

### Initial Response

Activate DDoS mitigation services immediately.
Contact ISP and DDoS protection providers.
Enable traffic filtering and rate limiting.
Document attack characteristics and timeline.

## Containment (15 minutes - 1 hour)

### Traffic Management

Implement traffic filtering at ISP level.
Enable DDoS protection services (CloudFlare, Akamai, etc.).
Configure rate limiting and traffic shaping.
Block known malicious IP addresses.

### Service Protection

Prioritize critical services and applications.
Implement emergency service degradation procedures.
Enable caching and content delivery networks.
Coordinate with hosting providers.

## Investigation (1-4 hours)

### Attack Analysis

Identify attack type (volumetric, protocol, application layer).
Analyze traffic patterns and sources.
Determine attack duration and intensity.
Assess impact on business operations.

### Threat Intelligence

Research attack attribution and motivation.
Check for similar attacks on industry peers.
Coordinate with threat intelligence services.
Document attack indicators and signatures.

## Recovery (4-12 hours)

### Service Restoration

Gradually restore services as attack subsides.
Monitor for attack resumption.
Validate service functionality and performance.
Remove temporary traffic restrictions.

### Capacity Planning

Assess infrastructure capacity and performance.
Implement additional DDoS protection measures.
Update network architecture for resilience.
Review and update service level agreements.

**Communication:**

- **Internal**
    - Keep leadership informed of attack status.
    - Coordinate with customer service and marketing.
    - Update IT operations and security teams.
    - Prepare internal communications.
- **External**
    - Notify customers of service disruptions.
    - Coordinate with ISP and DDoS protection providers.
    - Update website and social media status.
    - Consider law enforcement notification.

**Post-Incident**

Review DDoS protection effectiveness.
Implement improved monitoring and alerting.
Update incident response procedures.
Consider additional DDoS protection services.