YOUR LOGO

拒绝服务攻击（DDoS）：网络威胁与防御策略

2024

主讲人：郑冬贤

时间：2024

CONTENS

目录

YOUR LOGO

Part 01

DDoS攻击概述

DDoS攻击定义

DDoS攻击概念

DDoS（分布式拒绝服务）攻击是一种网络攻击手段，通过大量无用的请求拥塞目标服务器，导致其无法正常处理合法请求。

这种攻击方式使得目标服务器资源耗尽，无法为用户提供正常服务，甚至导致系统崩溃。

DDoS攻击特点

分布式攻击特性

DDoS攻击的特点是攻击源分布式，攻击者控制多台计算机同时发起攻击，难以追踪和防御。

攻击者通过控制大量“肉鸡”（被感染的计算机）对目标发起攻击，增加了攻击的隐蔽性和破坏力。

DDoS攻击影响

对企业的影响

企业可能面临客户流失和法律诉讼，长期影响企业的生存和发展。

DDoS攻击导致企业在线服务中断，造成直接的经济损失和品牌信誉损害。

YOUR LOGO

Part 02

DDoS攻击类型与实现方法

流量型攻击

UDP Flood攻击

01

攻击者发送大量UDP包到随机端口，消耗服务器资源，导致合法流量无法到达。

02

防御措施包括配置防火墙规则限制特定端口访问，监控网络流量识别异常模式。

协议型攻击

SYN Flood攻击

攻击者发送大量TCP连接请求而不完成握手，耗尽服务器TCP连接队列。

防御措施包括实施SYN cookies技术，减少半开连接对服务器资源的消耗。

应用层攻击

HTTP Flood攻击

模仿正常HTTP请求，但以极高频率进行，直接针对Web服务器或应用。

防御措施包括部署Web应用防火墙（WAF）识别和过滤异常请求。

YOUR LOGO

Part 03

DDoS攻击的防御策略

预防措施

增强网络基础设施

通过多线路接入、负载均衡等手段增强网络的抗攻击能力。

利用CDN和WAF等服务分散流量压力，提高网络的弹性和可用性。

检测措施

实时流量监控

- 实时监控网络流量，使用异常检测系统识别非正常流量模式。
- 集成日志管理和事件分析，快速识别潜在的DDoS活动。

响应措施

应急响应计划

制定详细的应急响应计划，确保快速有效地缓解攻击影响。

与ISP合作，在攻击发生时采取必要的流量清洗措施。

YOUR LOGO

Part 04

DDoS攻击的法律与伦理问题

法律问题

DDoS攻击的法律责任

DDoS攻击是违法行为，攻击者可能面临刑事责任和民事赔偿。

相关法律规定包括《计算机信息系统安全保护条例》、《网络安全法》等。

伦理问题

网络攻击行为违背了网络空间的伦理规范，应当受到道德谴责和法律制裁。

01. / 网络攻击的伦理规制

02. / 企业和个人应当遵守网络伦理，共同维护网络空间的安全和秩序。

YOUR LOGO

谢谢大家

2024

主讲人：郑冬贤

时间：2024