YOUR LOGO

ARP攻击的防范策略

2024

主讲人：郑冬贤

时间：2024

目录

YOUR LOGO

Part 01

ARP攻击原理与危害

ARP协议基础

01

ARP协议负责将IP地址映射为MAC地址，是网络通信的核心环节。

02

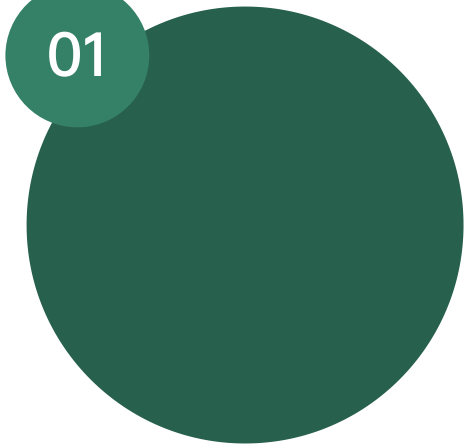
ARP协议的设计漏洞使其容易受到伪造报文的攻击。

ARP攻击手段

攻击者通过发送伪造的ARP报文，篡改受害者的ARP缓存，实现数据截获或网络中断。

ARP攻击后果

01



攻击成功可导致网络通信受阻，敏感信息泄露，如用户名、密码等。

YOUR LOGO

Part 02

ARP攻击的检测方法

手动检测方法

01

使用arp - a命令查看ARP缓存表，检查异常的IP- MAC映射关系。

主机级检测方法

01

被动检查系统接收到的ARP请求，主动探测发送ARP请求并验证响应的真实性。

网络级探测方法

配置主机定期向网管中心报告ARP缓存，查找报告信息的不一致性。

YOUR LOGO

Part 03

ARP攻击的防范措施

静态ARP绑定

01

在计算机上使用arp - s命令添加静态ARP缓存记录，避免动态学习导致的ARP欺骗。

使用ARP防火墙

部署专用ARP防护软件，如Anti- ARP，自动监测与阻止攻击。

划分虚拟局域网（VLAN）和端口绑定

01

根据ARP欺骗不会发生跨网段攻击的特点，将网络划分为多个网段，限制攻击影响范围。

YOUR LOGO

Part 04

增强网络设备安全性

启用ARP检测功能

现代交换机支持ARP检测功能，能够识别出不正常的ARP流量，有效防止ARP攻击。

部署ARP欺骗检测工具

部署专门的ARP欺骗检测工具，如Arpwatch、XArp等，及时发现异常ARP流量。

YOUR LOGO

Part 05

定期更新与维护

定期更新固件和软件

确保所有网络设备和计算机都安装了最新的安全补丁和更新。

网络隔离技术

01

通过VLAN或其他网络隔离技术，将敏感数据和关键设备与其他网络流量分开。

提高员工网络安全意识

定期举办网络安全培训和演习，提高员工对网络安全的意识。

YOUR LOGO

谢谢大家

2024

主讲人：郑冬贤

时间：2024