域名系统安全实验

金舒原
jinshuyuan@mail.sysu.edu.cn
计算机学院

提纲

1. 域名系统(DNS)概述
   - 认识域名-网络中主机的标识
   - 互联网域名空间
   - 域名数据库的内容
     - 资源记录
     - 区域
   - 互联网域名解析
   - DNS协议
2. 域名系统常见攻击、攻击原理及防护措施
   - 缓存污染攻击
   - 拒绝服务攻击
   - DNSSEC
   - 加密DNS协议
3. 实验说明
   - 实验目的和实验环境
   - 实验1: DNS缓存污染攻击
   - 实验2: DNS拒绝服务攻击

拒绝服务攻击

令服务器无法响应正常用户的请求

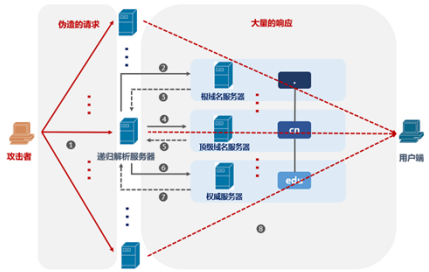
- DNS反射放大攻击
  - 攻击者利用开放的 DNS 服务器作为“反射器/反射放大器”，向目标服务器（受害者）发送大量DNS响应，造成网络拥塞，甚至瘫痪，无法响应正常用户请求。
- DNS查询洪泛攻击
  - 攻击者向目标 DNS 服务器发送大量 DNS 查询请求，导致目标服务器资源耗尽，无法响应正常的 DNS 查询请求。
- NXDomain 攻击
  - 攻击者向目标 DNS 服务器发送大量不存在的域名查询请求，导致目标服务器资源耗尽，无法响应正常的 DNS 查询请求。

提问：以上攻击，哪些是针对域名系统的攻击，哪些是利用域名系统特性构造的攻击?

拒绝服务攻击

典型攻击模型：反射放大攻击

- 利用开放的 DNS 服务器作为“**反射器**”
- 攻击者**伪造源地址为受害者**的DNS查询请求
- 利用**DNS响应报文大小远远大于请求报文**：查询具有数据量大的DNS响应报文的资源记录类型，如TXT记录或ANY记录



如何防止，缓解 DNS反射放大式拒绝服务攻击?

请讨论

5

提纲

1. 域名系统(DNS)概述
   - 认识域名-网络中主机的标识
   - 互联网域名空间
   - 域名数据库的内容
     - 资源记录
     - 区域
   - 互联网域名解析
   - DNS协议
2. 域名系统常见攻击、攻击原理及防护措施
   - 缓存污染攻击
   - 拒绝服务攻击
   - DNSSEC
   - 加密DNS协议
3. 实验说明
   - 实验目的和实验环境
   - 实验1: DNS缓存污染攻击
   - 实验2: DNS拒绝服务攻击

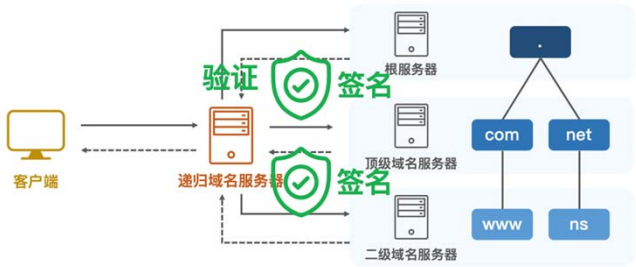
6

DNSSEC

基于数字签名算法，为域名响应报文提供完整性保障

- 域名所有者：对权威资源记录进行数字签名
- 域名服务器：对响应报文中的数字签名进行验证

验证不通过时，表示响应报文被篡改，即域名解析失败



加密DNS协议

在客户端和递归域名服务器间建立加密信道，传输域名解析报文

- 改变基于UDP协议的明文传输模式

  DoT（DNS over TLS）、DoH（DNS over HTTPS）

提供消息保密性和身份认证机制

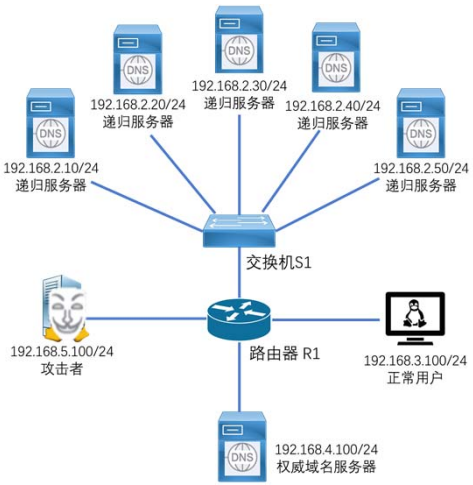
提纲

1. 域名系统(DNS)概述
   - 认识域名-网络中主机的标识
   - 互联网域名空间
   - 域名数据库的内容
     - 资源记录
     - 区域
   - 互联网域名解析
   - DNS协议
2. 域名系统常见攻击、攻击原理及防护措施
   - 缓存污染攻击
   - 拒绝服务攻击
   - DNSSEC
   - 加密DNS协议
3. 实验说明
   - 实验目的和实验环境
   - 实验1: DNS缓存污染攻击
   - 实验2: DNS拒绝服务攻击

实验2: DNS拒绝服务攻击

实验目的

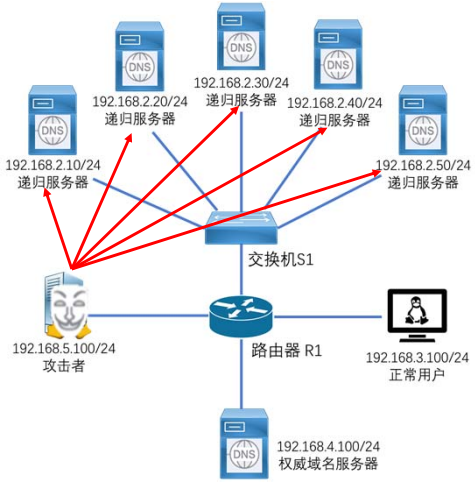
- 掌握DNS解析过程的工作原理及DNS报文结构
- 掌握DNS拒绝服务攻击原理、攻击过程及危害
- 思考并掌握DNS拒绝服务攻击的防御策略及技术



实验2: DNS拒绝服务攻击

实验内容

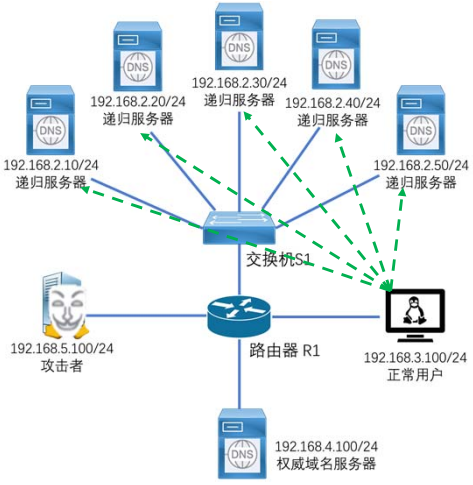
1. 编写攻击脚本。
2. 观察攻击效果
   (1)通过提高发包速率同时向多个递归服务器发起请求
   (2)在攻击者主机上查看发送的请求数据包大小
   (3)在受害者主机上查看其收到的DNS响应数据包大小
   (4)在受害者主机上，使用iftop命令查看攻击流量的大小
   (5)计算攻击流量放大的倍数，讨论实现DNS拒绝服务攻击的相关实验参数设置
   (6)重要实验过程和结果请截图，完成实验报告



实验2: DNS拒绝服务攻击

实验内容

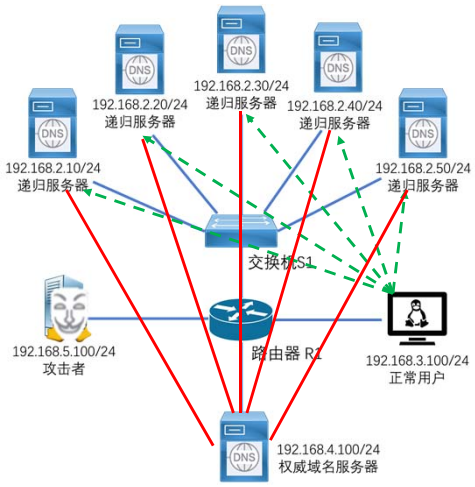
1. 编写攻击脚本。
2. 观察攻击效果
   (1)通过提高发包速率同时向多个递归服务器发起请求
   (2)在攻击者主机上查看发送的请求数据包大小
   (3)在受害者主机上查看其收到的DNS响应数据包大小
   (4)在受害者主机上，使用iftop命令查看攻击流量的大小
   (5)计算攻击流量放大的倍数，讨论实现DNS拒绝服务攻击的相关实验参数设置
   (6)重要实验过程和结果请截图，完成实验报告



实验2: DNS拒绝服务攻击

实验内容

1. 编写攻击脚本。
2. 观察攻击效果
   (1)通过提高发包速率同时向多个递归服务器发起请求
   (2)在攻击者主机上查看发送的请求数据包大小
   (3)在受害者主机上查看其收到的DNS响应数据包大小
   (4)在受害者主机上，使用iftop命令查看攻击流量的大小
   (5)计算攻击流量放大的倍数，讨论实现DNS拒绝服务攻击的相关实验参数设置
   (6)重要实验过程和结果请截图，完成实验报告

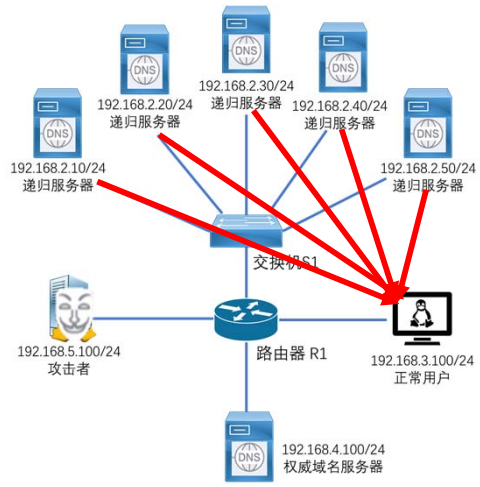


13

实验2: DNS拒绝服务攻击

实验内容

1. 编写攻击脚本。
2. 观察攻击效果
   (1)通过提高发包速率同时向多个递归服务器发起请求
   (2)在攻击者主机上查看发送的请求数据包大小
   (3)在受害者主机上查看其收到的DNS响应数据包大小
   (4)在受害者主机上，使用iftop命令查看攻击流量的大小
   (5)计算攻击流量放大的倍数，讨论实现DNS拒绝服务攻击的相关实验参数设置
   (6)重要实验过程和结果请截图，完成实验报告

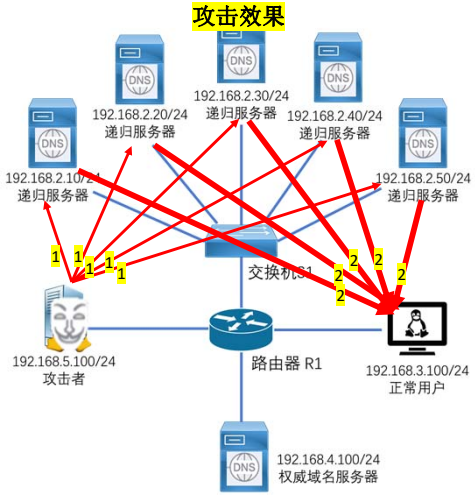


14

实验2: DNS拒绝服务攻击

实验内容

1. 编写攻击脚本。
2. 观察攻击效果
   (1)通过提高发包速率同时向多个递归服务器发起请求
   (2)在攻击者主机上查看发送的请求数据包大小
   (3)在受害者主机上查看其收到的DNS响应数据包大小
   (4)在受害者主机上，使用iftop命令查看攻击流量的大小
   (5)计算攻击流量放大的倍数，讨论实现DNS拒绝服务攻击的相关实验参数设置
   (6)重要实验过程和结果请截图，完成实验报告

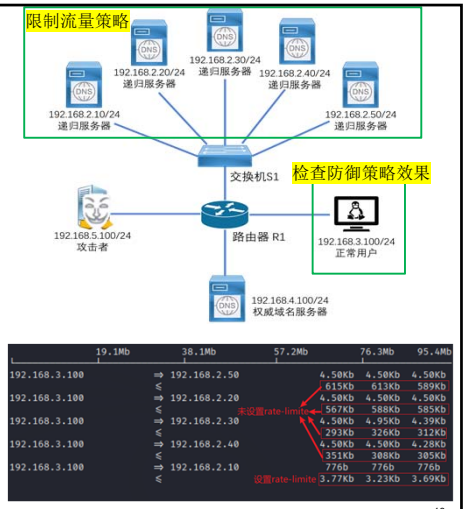


15

实验2: DNS拒绝服务攻击

实验内容

3. 防御DNS拒绝服务攻击
   (1)部署和配置限制流量防御机制
   (2)验证限制流量防御机制有效性
   (3)在受害者主机上检查限制流量防御效果
   (4)重要实验过程和结果请截图，完成实验报告
   (5)思考：
   除了限制流量策略，还有什么其他策略防范DNS拒绝服务攻击?



16