Misc 总结 ----流量分析 DNS认识

M1n3 / 2018-01-16 00:16:15 / 浏览数 3355 安全技术 CTF 顶(0) 踩(0)

网络协议—DNS

实验目的

了解DNS运作方式
掌握各种DNS记录的作用
学会使用wireshark分析DNS数据

实验环境

- 操作机：Windows XP
  - 实验工具：
    - Wireshark2.2

实验内容

DNS即Domain Name
System，域名系统，作为Internet的一个重要组成部分，和常用的协议。DNS采用53端口基于UDP协议，当数据量大时，采用TCP协议。DNS协议的作用是把域名解析到IP

实验一

了解常见DNS记录类型

方法一 了解DNS协议

可以对应如下DNS报文格式：

Transaction ID: 由生成DNS查询的程序指定的16位的标志符。该标志符也被随后的应答报文所用，申请者利用这个标志将应答和原来的请求对应起来.

flags：标志位，标记查询/应答，查询类型，截断，递归查询等等

DNS正文字段：

type：DNS记录类型，常用的有：

- A：A记录，指向别名或IP地址。
- NS：解析服务器记录。
- MX：邮件交换记录。
- CNAME：别名。
- AAAA：IPv6地址解析。
- txt：为某个主机名或域名设置的说明。
- PTR：指针记录，PTR记录是A记录的逆向记录。
- SOA：标记一个区的开始，起始授权机构记录。

方法二 分析DNS数据包

DNS应答：

查询sudalover.cn的DNSA记录，返回了sudalover.cn指向的一个别名：sudalover.cn.cdn.dnsv1.com，说明目标域名开启了CDN，然后CDN域名在解析直到ip地址。之所
下面是一个A记录指向ip地址的例子：

MX记录用于邮件交换，查询目标域名NX记录可以得知对方域名邮件服务指向。可以看出目标域名使用了QQ的邮件服务，并把自身的MX记录解析到了腾讯：

TXT记录，可以用来隐藏一些信息，常用于反垃圾邮件。

注释

DNS协议查询和应答字段往往会传输大量的数据，所以可以用于隐藏数据。在常见的CTF和网络安全的实际应用中，往往会出现DNS夹杂数据的情况出现。

DNS.pcapng.zip (0.001 MB) 下载附件
点击收藏 | 0 关注 | 1
上一篇：浅谈高级威胁情报对于安全建设的意义... 下一篇：Windows下的密码hash——...

1. 3 条回复


saviour2 2018-01-17 09:36:46

学习一下

0 回复Ta


1815837370479554 2018-05-29 14:02:44

学习一下

0 回复Ta


暮秋初九 2019-09-17 19:33:58

学习一下

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板