GFW与西厢计划

GFW的DNS欺骗攻击

写在前面

1. 本人在制作此PPT的过程中严格遵守了《计算机信息网络国际联网安全保护管理办法》相关规定
2. 对于PPT提到的对抗GFW的工具，本人仅进行了原理上的分析。
3. 本人将会彻底销毁本次实验中用到的工具，对此不愿接受任何质询。
4. 如有未尽事宜，本人对此PPT及内容享有最终解释权。

DNS污染的检测和防范

- [1]闫伯儒,方滨兴,李斌,王垚.DNS欺骗攻击的检测和防范[J].计算机工程,2006(21):130-132+135.

- 摘要：DNS是一个用于管理主机名字和地址信息映射的分布式数据库系统，它将便于记忆和理解的名称同枯燥的IP地址联系起来，大大方便了人们的使用。DNS是大部分网络应用的基础，但是由于协议本身的设计缺陷，没有提供适当的信息保护和认证机制，使得DNS很容易受到攻击。……由此可见防范对DNS的攻击，确保DNS系统的安全已经到了刻不容缓的地步。

DNS欺骗攻击原理

- 目前所有DNS客户端处理DNS应答包的方法都是简单地信任首先到达的数据包，丢弃所有后到达的，而不会对数据包的合法性作任何的分析。

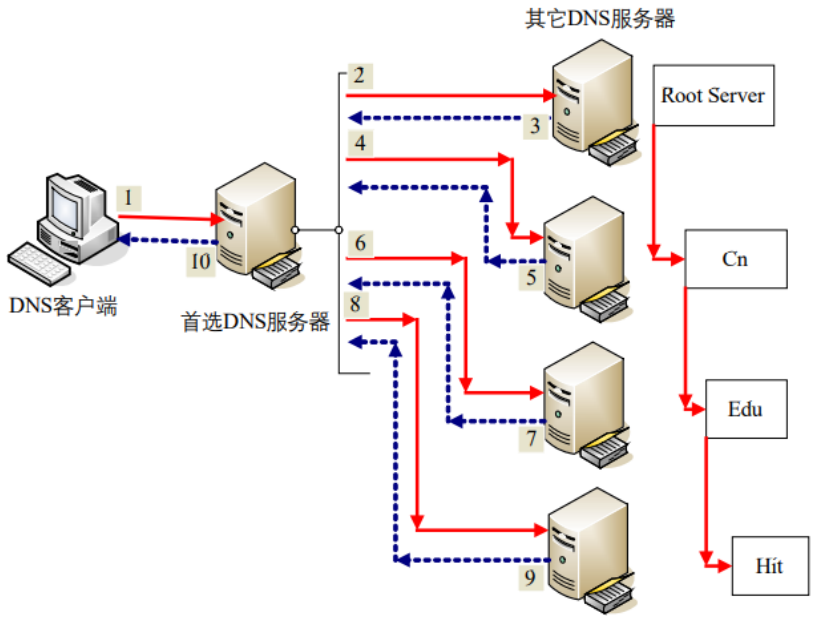

图 1 域名解析过程

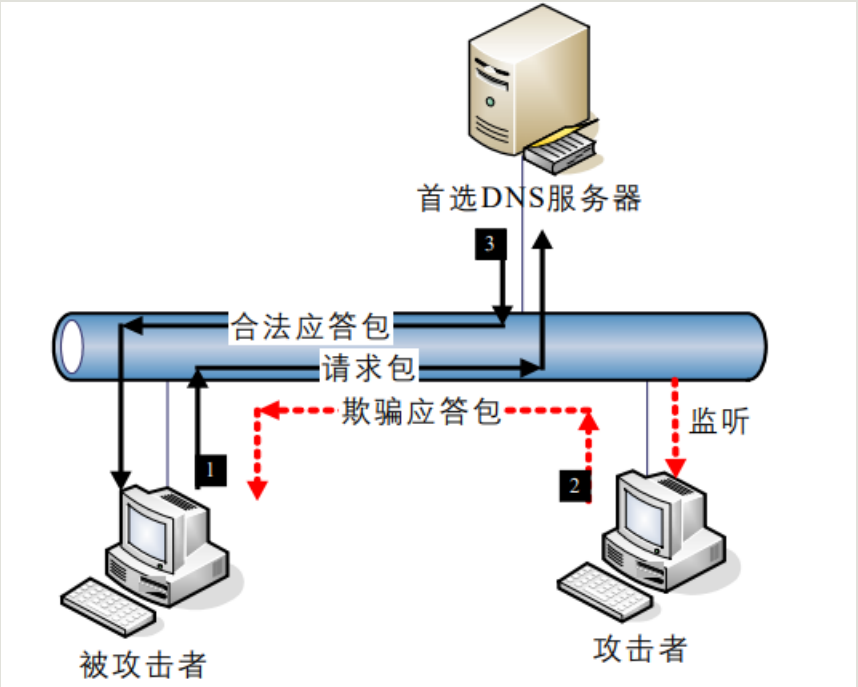

图 2 DNS 欺骗攻击

DNS欺骗攻击的检测

- 被动监听检测：
  - DNS服务器不会给出多个结果不同的应答包，即使目标域名对应多个 IP 地址，DNS服务器也会在一个DNS应答包中返回，只是有多个应答域(Answer Section)而已。
- 虚假报文探测：
  - 如果向一个非DNS服务器发送请求包，正常来说不会收到任何应答，如果收到了应答包，则说明受到了攻击。
- 交叉检查查询：
  - 在客户端收到 DNS 应答包之后，向 DNS 服务器反向查询应答包中返回的 IP 地址所对应的 DNS 名字。

校园网DNS污染检测

- 环境：
  - 操作系统：windows 10
  - 网络：NJU-WLAN
  - 浏览器：Chrome
  - 抓包工具：Wireshark

- 结论：
  1. 南京大学DNS服务器(210.28.129.251)存在DNS污染现象。
  2. 使用境外DNS服务器(8.8.8.8, 199.85.126.10)会受到DNS欺骗攻击。
  3. 攻击者并没有试图掩盖自己的DNS欺骗攻击行为。
  4. 在国内基本不存在合法的方式能够获得正常的DNS解析服务(114.114.114.114也一样无法解析)。
  5. “由此可见防范对DNS的攻击，确保DNS系统的安全已经到了刻不容缓的地步。”——方滨兴

检测数据的分析

- 环境：
  - DNS服务器：校园网DNS(210.28.129.251)
  - 尝试进行的DNS查询：www.google.com
- 查询结果：
  - 90 Standard query response 0x963e A www.google.com A 31.13.69.86
  - 只收到了一个包（并未直接攻击我们的客户端）
  - IP反查(IP138.com)：
    - onedrive.live.com
    - www.tumblr.com
    - www.epochtimes.com
    - www.google.com
    - t66y.com
  - 无法通过交叉检查查询验证

检测数据的分析

- 环境：
  - DNS服务器：谷歌DNS(8.8.8.8)
  - 尝试进行的DNS查询：www.google.com
- 查询结果：
  - 90 Standard query response 0x7b40 A www.google.com A 157.240.1.33
  - 只收到了一个包（诡异？）
  - IP反查(IP138.com)：
    - onedrive.live.com
    - www.tumblr.com
    - www.epochtimes.com
    - www.google.com
    - t66y.com
  - 无法通过交叉检查查询验证

检测数据的分析

- 环境：
  - DNS服务器：诺顿DNS(199.85.126.10)
  - 尝试进行的DNS查询：www.google.com
- 查询结果：
  - 90 Standard query response 0xd0f7 A www.google.com A 157.240.10.36
  - 90 Standard query response 0xd0f7 A www.google.com A 108.160.165.53
  - 90 Standard query response 0xd0f7 A www.google.com A 142.250.72.196
  - 收到了3个包（？？？）
  - IP反查(IP138.com)：
    - 略
  - 无法通过被动监听检测，交叉检查查询验证 。

检测数据的分析

- 环境：
  - DNS服务器：无(随意将DNS服务器设为142.146.254.142)
  - 尝试进行的DNS查询：www.google.com
- 查询结果：
  - 90 Standard query response 0xe4f6 A www.google.com A 118.193.202.219
  - 90 Standard query response 0xe4f6 A www.google.com A 202.160.128.96
  - 收到了2个本不该存在的包
  - IP反查(IP138.com)：
    - 略
  - 无法通过被动监听检测，虚假报文探测，交叉检查查询验证 。
  - 我们压根就没打算瞒着你.....

Play a Joke on GFW

- DNS 攻击指向的IP是固定且有限的：
  - 如果一直尝试请求www.google.com，DNS返回的IP地址有且仅有那几个。
  - 如果反向查询DNS返回的错误的IP地址，我们可以得到其它被污染的网址。

- 搜索：
  - 首先指定一组初始网址（DNS攻击比较严重的），以较大的权值初始化一个字典。
  - 循环：
    - 从字典中选取当前权值最大的网址。
    - 对该网址进行DNS请求，并进行反查。
    - 将反查的所有的网址在字典中的权值加1。
  - 返回最后更新过的字典。

对结果的分析：

- 墙是有意识的：
  - 当你不断地发送如上请求，墙会从开始的认真欺骗到最后的随意糊弄。
  - 这样其实不大容易高效地完成搜索。
- 墙的DNS污染的网址数是有限的：
  - 在GFWlist中，DNS污染的网址只有一部分，除了DNS污染外，墙还有多种多样的方式让你访问不了你想访问的网站。
  - 我们也并不能保证所有被DNS污染的网址都能被这种方式找到：
    - 可能不同地方的DNS污染程度不同。
    - 可能不同被DNS污染的网址并不具有我们描述的关系，虽然使用多起点BFS可能能稍好地解决这个问题。
- 墙是有一定积极意义的？—通过这种方式找到的被DNS污染的网址中有一多半是成人网站。