DNS缓存投毒攻击

定义：攻击者欺骗DNS服务器相信伪造的DNS响应的真实性。

原理：向DNS缓存服务器发送不存在地址的DNS请求，然后伪造DNS主服务器向DNS缓存服务器应答，从而把此ip地址映射到自己伪造的地址上。

我们首先来分析dns服务器对不存在网址的正常解析过程：

1）客户端向DNS缓存服务器发送对[www.xoxox.org](http://www.xoxox.org)（某不存在的网址）的DNS查询请求。

2）当DNS缓存服务器上没有www.xoxox.org对应的IP地址，则DNS缓存服务器就会通过迭代的方法最后询问DNS主服务器上保存的www.xoxox.org对应的IP地址。

3）DNS主服务器响应DNS缓存服务器的请求，返回www.xoxox.org对应的IP地址。

4）DNS缓存服务器收到DNS主服务器的应答后，把应答消息转发给客户端。

5）客户端通过该ip地址访问[www.xoxox.org](http://www.xoxox.org)。

这就意味着，攻击方只要伪造响应报文给DNS缓存服务器，DNS缓存服务器上就记录了错误的域名到IP地址的对应关系，然后DNS缓存服务器把这个错误的对应关系发给客户端，就可以让他访问攻击方指定的ip地址。

由此，可得攻击过程如下：

1）客户端向DNS缓存服务器发送对[www.xoxox.org](http://www.xoxox.org)（某不存在的网址）的DNS查询请求。

2）当DNS缓存服务器上没有www.xoxox.org对应的IP地址，则DNS缓存服务器就会通过迭代的方法最后询问DNS主服务器上保存的www.xoxox.org对应的IP地址。

3）在DNS主服务器还未返回给DNS缓存服务器时，攻击方发送响应报文，使之与已发送的dns查询报文的报头ID匹配（DNS报头的ID号是 16位2进制，命中率是1/65536），把错误的域名到IP对应关系告诉DNS缓存服务器，这就是给DNS缓存服务器的一次投毒。

4）DNS缓存服务器把攻击方的应答当成DNS主服务器的应答，并把应答消息转发给客户端。

5）客户端通过该ip地址访问[www.xoxox.org](http://www.xoxox.org)，却进入了攻击方指定的网址。

防护：

1. 部署多台dns权威服务器，降低攻击效率。
2. 使用**DNS ”源端口随机性”较好的软件或者版本，降低投毒命中率。**
3. **使用dnssec协议，使攻击者无法伪造响应报文，而且杜绝了dns缓存投毒攻击。**