基于 Web 的 DNS 欺骗技术研究

张尚韬

（福建信息职业技术学院，福建 福州 350003）

摘 要：本文根据 DNS 解析的过程，结合 DNS 协议本身的缺陷，总结分析了 DNS 欺骗的原理，利用 DNS 信息劫持进行 DNS 欺骗。当客户端发送域名解析请求时，先于 DNS 服务器给客户端发送欺骗应答数据包，由于客户端处理 DNS 应答报文都是简单地信任先到达的数据包，只要 DNS 应答数据包的序列号标识与请求数据包的序列号标识匹配就可以把客户端的请求重定向到某个预先设定的网页。并基于此设计开发了局域网的 DNS 欺骗系统。

关键词：DNS 欺骗；重定向；系统

中图分类号：TP393 **文献标识码：**A **文章编号：**1008-2395(2012)03-0024-06

收稿日期：2012-02-27

作者简介：张尚韬（1980-），讲师，硕士，研究方向：计算机网络技术。

Internet 在当今社会展示了巨大的魅力，越来越多的用户通过网络获取信息，而 Web 攻击者千方百计通过这些信息引诱用户去访问并点击他设定的 Web 陷阱，研究 TCP/IP 协议[1]的安全缺陷和 DNS[2]网络欺骗攻击的技术原理，对了解网络协议，增强安全防范意识，对安全缺陷采取积极的防御措施，以及下一代网络及无线网络的发展在可靠性、优良性和抗攻击性上有重要价值。

1 DNS 欺骗概述

DNS（Domain Name System，域名系统）是因特网的一项核心服务，是一个用于管理主机名字和地址映射的分布式数据库，它将便于记忆和理解的名称同枯燥的 IP 地址联系起来，能够使人更方便的访问 Internet，而不用去记住能够被机器直接读取的 IP 数串。

DNS 欺骗即域名信息欺骗是最常见的 DNS 安全问题。所谓 DNS 欺骗，就是伪装 DNS 服务器提前向客户端发送响应数据包，使客户端 DNS 缓存中域名所对应的 IP 就是攻击者自定义的 IP 了，同时客户端也进入攻击者指定的网站。当一个 DNS 服务器掉入陷阱，使用了来自一个恶意 DNS 服务器的错误信息，那么该 DNS 服务器就被欺骗了。DNS 欺骗会使那些易受攻击的 DNS 服务器产生许多安全问题，例如：将用户引导到错误的 Internet 站点等。

本文主要利用 DNS 信息劫持进行 DNS 欺骗。DNS 欺骗的具体攻击过程如图 1 所示。

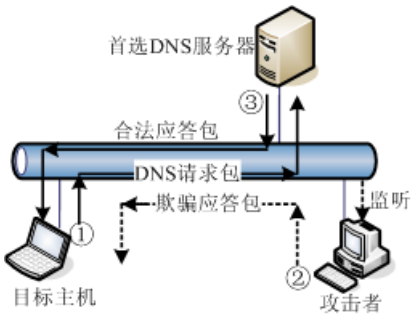

图 1 DNS 欺骗攻击示意图

以福州大学网站 www.fzu.edu.cn 为例，假设伪造的 IP 为 1. 2. 3. 4，则具体的欺骗过程如下：

(1)DNS 客户端向首选 DNS 服务器发送对于 www.fzu.edu.cn 的递归解析请求数据包①。

(2)攻击者监听到请求，并根据请求 ID 构造发送欺骗应答包②，通知与 www.fzu.edu.cn 对应的 IP 地址为 1.2.3.4。

(3)本地 DNS 服务器返回正确应答(合法应答数据包③)，如果晚于攻击者的应答，则此应答数据包被丢弃；如果早于攻击者的应答，则攻击者的应答数据包被丢弃。

(4)如果(3)中判断的为攻击者的 DNS 应答数据包先到达，则欺骗成功，客户端对 www. fzu. edu.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

cn 的访问被重定向到 1. 2. 3. 4。

2　DNS 欺骗系统的设计及实现

2.1　DNS 欺骗系统设计

设计一个 DNS 欺骗系统，基于 DNS 欺骗的原理，当客户端访问指定的域名（一般为门户网站或百度等搜索引擎）时，构造 DNS 欺骗数据包，重定向[3]客户端的访问。欺骗的方法是：把预先设定的网页作为中间过程，在其脚本语言中让客户端以 IP 的形式重新与他访问的网站进行连接，如果中间过程时间很短，就可以达到欺骗客户端的目的而不被发现。DNS 欺骗系统包括软件模块和模块间的控制关系和模块组成关系，在设计阶段，模块指功能模块，即按设计原理，划分独立功能而设计的模块。软件结构用模块结构图表示。模块结构图的方框表示模块，分支表示调用关系或组成关系，即上层模块调用下层模块，或上层模块由下层模块组成。DNS 欺骗系统模块设计如图 2。

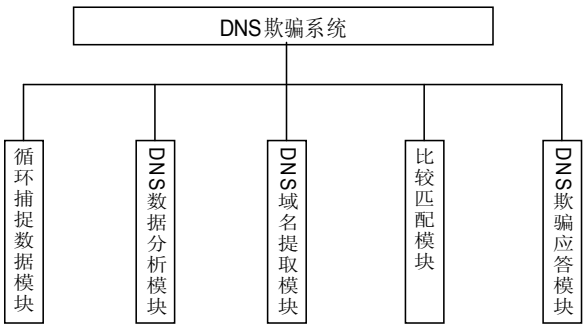

图 2　DNS 欺骗系统模块设计图

DNS 欺骗系统模块功能如下:

(1)循环捕获数据模块

循环捕获数据模块模块的主要功能为循环捕捉数据，具体的说就是时刻监听网络中的 DNS 查询数据包，一旦捕获 DNS 请求数据就转入下个模块进行处理，没有捕获则循环进行监听。

(2)DNS 数据分析模块

DNS 数据分析模块的目标就是把 DNS 查询数据包输入到模块之后，解析 DNS 数据包的各个主要字段。具体的说分为两个方面：一是为 DNS 域名提取模块提供 DNS 域名查询的数据，二是当客户端查询的域名与非法域名数据库中的域名相匹配时，为欺骗应答模块提供 DNS 应答数据包所需的各项置换和替换的数据，其中包括 DNS 查询序列号标识、查询问题及 IP 和端口等数据，为快速应答处理做好数据准备。

(3)DNS 域名提取模块

DNS 域名提取模块的主要功能为提取 DNS 查询数据包中的域名字段。但是 DNS 查询数据包中的域名字段长度是不固定的，可以通过 DNS 查询数据包的长度计算出 DNS 查询域名的长度，然后进行提取。

(4)比较匹配模块

比较匹配模块主要功能是比较 DNS 查询的域名是否与配置文件信息中需要攻击的域名相匹配，匹配则调用欺骗应答模块构造 DNS 欺骗应答数据包，重定向客户端的访问。

(5)DNS 欺骗应答模块

DNS 欺骗应答模块的功能就是快速构造与 DNS 查询数据包序列号匹配的欺骗应答数据包，若在合法 DNS 服务器返回响应数据包之前到达客户端，则合法响应报文被丢弃，客户端查询的域名就被解析为自定义的 IP。

2.2　DNS 欺骗系统实现

2.2.1　DNS 欺骗系统实现流程

DNS 欺骗系统在监控主机（攻击主机）上运行，是基于 Linux 系统开发的系统，需要安装 Libpcap 库和搭建 HTTP 服务器。系统的网络环境为：共享式以太网，攻击主机处于旁路监听模式[4]。共享式以太网，即局域网的出入口为具有镜像端口的交换机，而运行 DNS 欺骗系统的主机接入到交换机的镜像端口上，从而捕获该局域网的所有数据包。DNS 欺骗系统实现流程如图 3

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

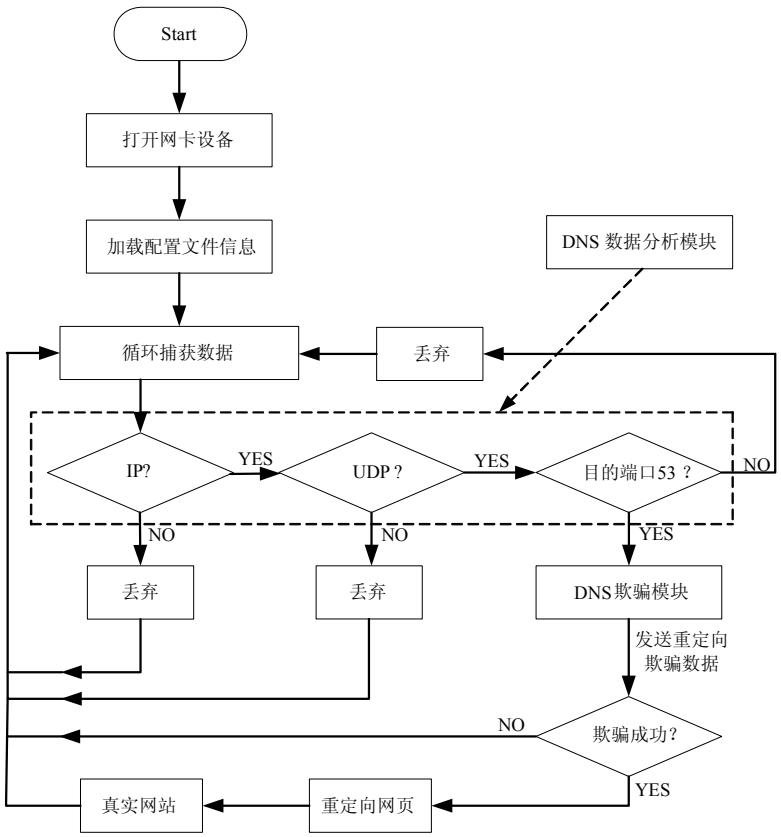

图 3　DNS 欺骗系统实现流程

DNS 欺骗系统是基于 Linux 系统设计的，它利用 Libpcap 库[5]捕获和过滤数据，在捕获处理数据之前需要从配置文件中读取数据，配置的参数有目标主机 IP、攻击的域名地址和重定向欺骗的 IP 地址（即 HTTP 服务器的 IP 地址）等。利用 Libpcap 库函数捕获网络中的数据包，把网卡设置为混杂模式，先根据以太网首部中的帧类型字段判断协议类型（0x0800 为 IP 数据包），再根据 IP 首部中的 8 位协议字段判断传输层的协议。因为 DNS 数据包是基于 UDP 的数据包，所以只需要处理 UDP 数据包，其它类型的直接丢弃。再从 UDP 数据包中分离出 DNS 查询报文，即目的端口为 53 的 UDP 数据包，将其送入 DNS 欺骗模块进行处理，继续处理下一个数据包。

2.2.2　DNS 欺骗系统主要模块实现思路

DNS 欺骗系统的实现思路是：利用旁路接入模式监听局域网中的数据包，当发现有客户端发送 DNS 查询数据包（UDP：目的端口 53），则提取其域名字段内容，与配置文件信息中的攻击域名地址进行比较，如果匹配，则根据 DNS 查询数据包的序列号标识构造 DNS 欺骗应答数据包，如果先于合法应答数据包到达客户端，则其访问就被重定向到预先设定的网站。

提取域名字段内容、域名攻击判断、构造数据包、发送重定向数据包等功能都是由 DNS 欺骗系统来实现的。DNS 欺骗系统的详细功能实现如图 4 中的虚线框所示。

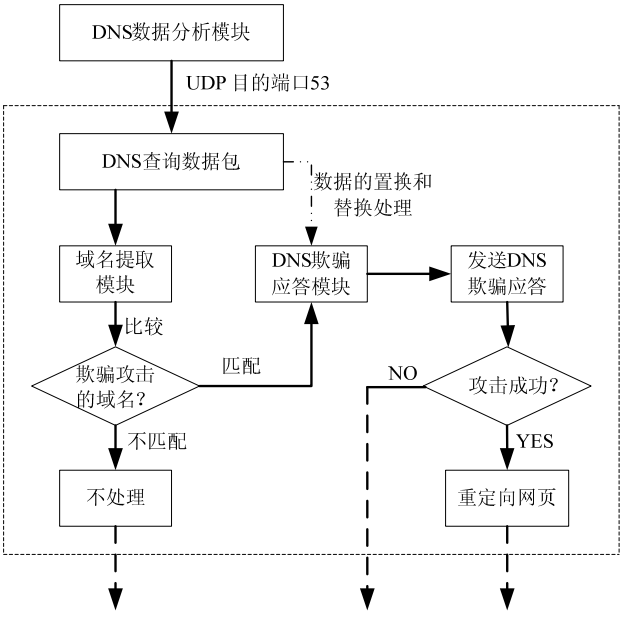

图 4　DNS 欺骗系统详细功能实现图

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

3　DNS 欺骗系统的测试与结果分析

实验环境利用了福建信息职业技术学院网络设备实验室的局域网环境，局域网内的计算机通过非智能交换机相连，这时候需要人为的进行旁路设置，一般情况下，利用一台 Hub 来实现。将网关设备、内网交换机、监控机（攻击主机）和目标主机都接在这台 Hub 上，因为 Hub 是介质共享的，所以监控机也能得到全部被监控主机的通信数据，网络拓扑如图 5 所示。这种情况下也可以把 Hub 换成可以做镜像端口的交换机。

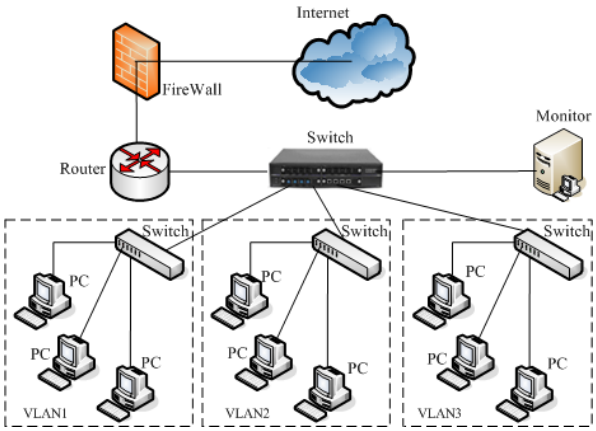

图 5　测试网络拓扑

当客户端访问指定的域名（一般为门户网站或百度等搜索引擎）时，构造 DNS 欺骗数据包，把客户端的访问重定向到预先设定的恶意网页作为中间过程，当完成该网页的请求时，客户端会以 IP 的形式跳转到客户端访问的网站，达到欺骗的目的。

某次测试参数设置：目标主机 IP 为 192.168.3.70（或者是某一网段的 IP），监控主机 IP 为 192.168.3.111，DNS 欺骗的域名为 www.baidu.com，DNS 域名欺骗后指向 IP 设置为为 192.168.3.111。启动“科来”网络分析系统监听数据包，分析 DNS 欺骗[6]的过程。

某次测试的流程如下：首先运行监控机（攻击主机）上的欺骗系统，导入配置文件信息（包括目标主机 IP、监控主机 IP 和欺骗的域名信息），选择监控机的真实网络适配器 eth0 捕获数据包，设置过滤规则为仅捕获 192.168.3.70：53（UDP）数据包，欺骗系统运行后处于监听状态，如图 6 为 DNS 欺骗系统的初始运行状态。

```
[root@localhost html]# ./dnsspoof
udp and host 192.168.3.70 and dst port 53Device: eth0
Listening on...
```

图 6　DNS 欺骗系统初始运行状态

当监控主机捕获到数据包时，就会调用 DNS 数据分析模块分析数据包是否为 DNS 查询数据包，若是，与配置文件信息中需要欺骗的域名比较，匹配的话，发送 DNS 欺骗数据包，重定向客户端的访问。在欺骗系统启动后，目标主机 192.168.3.70 分别访问了不同的网页。图 7 显示的是 DNS 欺骗系统捕获到目标主机访问 www.baidu.com，并发送 DNS 欺骗数据包的过程。

```
[root@localhost html]# ./dnsspoof
udp and host 192.168.3.70 and dst port 53Device: eth0
Listening on...
capture the dns packet!
+ DNS query [www.google.cn] from 192.168.3.70
capture the dns packet!
+ DNS query [www.baidu.com] from 192.168.3.70
+ DNS response [192.168.3.111] to 192.168.3.70
capture the dns packet!
+ DNS query [pingfore.qq.com] from 192.168.3.70
capture the dns packet!
+ DNS query [trace.qq.com] from 192.168.3.70
capture the dns packet!
+ DNS query [huoju.icoke.qq.com] from 192.168.3.70
capture the dns packet!
+ DNS query [stock1.finance.qq.com] from 192.168.3.70
```

图 7　DNS 欺骗系统的运行状态

其中目标主机访问谷歌和腾讯的网站，不是欺骗系统需要欺骗的域名，没有对此 DNS 查询数据包处理；当目标主机访问百度时，DNS 欺骗系统对客户端进行了重定向欺骗，目标主机先访问攻击主机（192.168.3.111）设定的中间网页，之后以 IP 的形式访问百度（220.181.37.55 为百度的一个服务器的 IP 地址）。如图 8 显示的是对目标主机欺骗跳转后的结果。

图 8　DNS 域名欺骗的结果

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

“科来”网络分析系统也捕获到客户端访问网页（DNS 域名解析）、DNS 欺骗系统发送欺骗数据包和以 IP 形式跳转的过程。如图 9 所示。图中第一列为数据包编号，第二列为数据包的捕获时间，第三列为数据包源 IP，第四列为数据包目的 IP，第五列为 TCP 数据包的标志位，第六列为数据包的概要内容。

从图 9 中可以看出，数据包 80 为目标主机向首选 DNS 服务器（202.115.32.36）查询百度(需要欺骗的域名)的 IP 地址。当 DNS 欺骗系统捕获到数据包 80 时，立即构造 DNS 欺骗数据包，假冒首选 DNS 服务器把 www.baidu.com 对应的 IP 地址设置为 192.168.3.111，即图 9 中的数据包 81。真正的首选 DNS 服务器 202.115.32.36 的应答为图 9 中的数据包 82。

从图 9 数据包的绝对时间可以看出数据包 81 比数据包 82 先到达客户端 192.168.3.70，则客户端访问的 www.baidu.com 就被重定向到 192.168.3.111。由于所有 DNS 客户端处理 DNS 应答报文都是简单的信任首先到达的数据包，丢弃所有后到达的，而不对数据包的合法性做任何的分析，所以数据包 82 被客户端丢弃，不做任何处理。

数据包 83、84、85 为客户端与 HTTP 服务器（192.168.3.111）三次握手建立连接的过程，数据包 86~96 为中间网页的下载过程，93~96 为完成页面下载双方端口关闭连接的过程；数据包 107~115 为客户端以 IP 形式连接其请求的真实网站的过程（本测试中为客户端以 220.181.37.55 连接百度），如图 10 所示。

编...	绝对时间	源	目标	TCP:标志	概要
80	16:16:58.112573	192.168.3.70:1030	202.115.32.36:domain		C: Q=www.baidu.com.(A)
81	16:16:58.113064	202.115.32.36:domain	192.168.3.70:1030		S: Q=www.baidu.com.(A) A=192.168.3.111
82	16:16:58.115359	202.115.32.36:domain	192.168.3.70:1030		S: Q=www.baidu.com.(A) A=211.94.144.100
83	16:16:58.121547	192.168.3.70:2687	192.168.3.111:www-http	..00 0010	序列号=4056952299,确认号=0000000000,标志=....S...
84	16:16:58.122023	192.168.3.111:www-http	192.168.3.70:2687	..01 0010	序列号=3157903275,确认号=4056952300,标志=.A..S...
85	16:16:58.122066	192.168.3.70:2687	192.168.3.111:www-http	..01 0000	序列号=4056952300,确认号=3157903276,标志=.A.....
86	16:16:58.124302	192.168.3.70:2687	192.168.3.111:www-http	..01 1000	C: GET / HTTP/1.1
87	16:16:58.124865	192.168.3.111:www-http	192.168.3.70:2687	..01 0000	序列号=3157903276,确认号=4056952582,标志=.A.....
88	16:16:58.127484	192.168.3.111:www-http	192.168.3.70:2687	..01 0000	S: HTTP/1.1 200 OK
89	16:16:58.128714	192.168.3.111:www-http	192.168.3.70:2687	..01 0000	S: HTTP流还有1460字节的数据
90	16:16:58.128739	192.168.3.70:2687	192.168.3.111:www-http	..01 0000	序列号=4056952582,确认号=3157906196,标志=.A.....
91	16:16:58.130401	192.168.3.111:www-http	192.168.3.70:2687	..01 0000	S: HTTP流还有1460字节的数据
92	16:16:58.130434	192.168.3.70:2687	192.168.3.111:www-http	..01 0000	序列号=4056952582,确认号=3157907656,标志=.A.....
93	16:16:58.131316	192.168.3.111:www-http	192.168.3.70:2687	..01 1001	S: HTTP流还有733字节的数据
94	16:16:58.131386	192.168.3.70:2687	192.168.3.111:www-http	..01 0000	序列号=4056952582,确认号=3157908390,标志=.A.....
95	16:16:58.166089	192.168.3.111:www-http	192.168.3.70:2687	..01 0001	序列号=4056952582,确认号=3157908390,标志=.A.....
96	16:16:58.166566	192.168.3.111:www-http	192.168.3.70:2687	..01 0000	序列号=3157908390,确认号=4056952583,标志=.A.....

图 9　DNS 欺骗系统对 DNS 数据包的处理

编...	绝对时间	源	目标	TCP:标志	概要
107	16:16:58.734281	192.168.3.70:2691	220.181.37.55:www-http	..00 0010	序列号=3973777974,确认号=0000000000,标志=....S...
108	16:16:58.778571	220.181.37.55:www-http	192.168.3.70:2691	..01 0010	序列号=2232822970,确认号=3973777975,标志=.A..S...
109	16:16:58.778636	192.168.3.70:2691	220.181.37.55:www-http	..01 0000	序列号=3973777975,确认号=2232822971,标志=.A.....
110	16:16:58.780922	192.168.3.70:2691	220.181.37.55:www-http	..01 1000	C: GET / HTTP/1.1
111	16:16:58.848124	220.181.37.55:www-http	192.168.3.70:2691	..01 0000	序列号=2232822971,确认号=3973778385,标志=.A.....
112	16:16:58.850569	220.181.37.55:www-http	192.168.3.70:2691	..01 1000	S: HTTP/1.1 200 OK
113	16:16:58.852702	220.181.37.55:www-http	192.168.3.70:2691	..01 0000	S: 继续或非HTTP通信, 1420 字节的二进制数据
114	16:16:58.852776	192.168.3.70:2691	220.181.37.55:www-http	..01 0000	序列号=3973778385,确认号=2232824763,标志=.A.....
115	16:16:58.852795	220.181.37.55:www-http	192.168.3.70:2691	..01 1000	S: 继续或非HTTP通信, 87 字节的二进制数据

图 10　客户端以 IP 形式连接其请求的真实网站

在局域网的中小流量的网络环境下，经过上面的测试分析，可以知道当目标主机访问配置文件中的攻击域名时，DNS 欺骗系统成功地把客户端重定向到预先设定的中间网页，当客户端下载完中间网页时，又根据其脚本语言的指令以 IP 的形式跳转到客户端访问的网站。因为攻击的域名一般为门户网站或百度等搜索引擎，这些站点是客户端信任的站点，所以对于一般用户而言，浏览器的地址栏出现 IP 的形式也不会怀疑，这样就达到了欺骗的目的。

4　总结

堡垒最容易从内部攻破。据调查统计，已发

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

生的网络安全事件中，70%的攻击是来自内部，因此网络安全不仅仅是对外的，内部网络的欺骗攻击行为成为内部网络安全研究的重点。通过研究 DNS 欺骗技术，将来可以为拥有中小型网络的企事业单位提供全方位的内部网络非法网站访问监控服务。

参考文献：

[1] W RICHARD STEVENS. TCP/IP 详解卷 1：协议[M]. 北京:机械工业出版社, 2005: 101-110.

[2] DECCIO, CASEYSEDAYAO. Quantifying DNS namespace influence[J]. Computer Networks, 2012, 56(2): 780-794.

[3] 杨青. 基于蜜罐的网络动态取证系统研究[J]. 山东科学, 2010(5): 59-65.

[4] 宋广军. 基于校园网的防火墙和入侵检测联动技术研究[J]. 科技资讯, 2011(34): 25.

[5] 张毅. 基于 Libnet 和 Libpcap 的网络丢包率测试平台设计[J]. 广东通信技术, 2010(1): 23-27.

[6] 孔政, 姜秀柱. DNS 欺骗原理及其防御方案[J], 计算机工程, 2010, 36(03): 125-127.

A **Study of DNS Spoofing Technology Based on Web**

ZHANG Shang-tao

(Fujian Polytechnic of Information Technology, Fuzhou 350003, China)

Abstract: According to the DNS resolution process and the drawback of DNS itself, this paper analyses the principle of DNS spoofing and DNS information hijack.When the client sends a domain resolution query, it will send the spoofing response packet to the client ahead of the DNS server. Since the way of the client processing DNS response is to trust the first arrival data simply, the client query can be redirected to malicious Web site only by matching the ID of the response with the ID of the query. This paper designs and develops DNS spoofing system based on LAN.

Key words: DNS spoofing; redirection; system

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net