

基于 DNS 重定向技术的网络安全审计系统

殷 俊 王海燕 潘显萌
(公安部第三研究所 上海 201204)

摘 要 网络安全审计是网络管理的重要任务,是保障网络安全、稳定运行的重要方法。针对网络安全审计系统部署复杂、成本较高的问题,提出一种利用 DNS 重定向技术进行网络安全审计的方法。通过修改网关 DNS 配置,重定向网络数据流,在不改变网络结构和客户端配置的情况下,即可对网络数据进行行为审计。实验结果表明,该种审计方案安装简便、成本较低,有助于小型网络管理者增强安全防范能力及提高网络管理水平。

关键词 网络安全审计,重定向,透明代理

中图法分类号 TP309 文献标识码 A

Network Security Audit System Based on Redirection of DNS

YIN Jun WANG Hai-yan PAN Xian-meng

(The Third Institute, Ministry of Public Security, Shanghai 201204, China)

Abstract Network security auditing is an important task of network management, and it is also an important way to ensure network security and stability. Common network security audit system is complex and high cost. In view of this, we proposed a network security audit system based on redirection of DNS. The method by modifying the DNS configuration in gateway can monitor the data without changing the structure of the network or the configuration of clients. Experimental results show that it is simple, low cost and helpful for administrators to improve their capability of network management.

Keywords Security audit, Redirection, TransProxy

国际标准化组织(ISO)对网络安全审计的功能定义为:对与安全有关的活动的信息进行识别、记录、存储和分析;审计的记录用于检查网络上发生了哪些与安全有关的活动,谁(哪个用户)对这个活动负责,主要功能包括:安全审计自动响应、安全审计数据生成、安全审计分析、安全审计浏览、安全审计时间存储、安全审计事件选择等^[1]。

据统计,来自内部网络的入侵和破坏占网络安全事件的半数以上。由于内部人员本身就具有一定的权限和密码,因此即便没有掌握深层次的技术,也能够对网络造成巨大的破坏。而传统的网络安全审计系统硬件价格较高、部署安装较复杂,对一般的小型网络管理者来说使用成本过大。

因此本文设计并实现了一种通过几款开源软件的组合应用,依托 DNS 重定向技术,利用一台接入局域网的台式电脑,即可对整个局域网的网络流量进行网络安全审计的方法。该方

法为小型网络管理者提供了一种低成本的网络安全审计方案。

1 关键技术理论研究

1.1 DNS 域名系统

英特网上的服务器通过 IP 地址来确定唯一性,但由于 IP 地址不便于记忆,因此引入了 DNS 域名解析系统作为域名和 IP 地址相互映射的一个分布式数据库,以方便用户更快速地访问互联网服务器^[2]。域名可将一个 IP 地址关联到一组有意义的字符上。用户访问一个网站时,既可输入该网站的 IP 地址,也可输入其域名,对访问者而言,两者是相同的。例如:百度公司的 Web 服务器的 IP 地址是 115.239.211.112,这个 IP 对应的域名是 www.baidu.com,因此不管用户在浏览器中输入的是 115.239.211.112 还是 www.baidu.com,都可以打开并访问其 Web 网站。

```
637 18.29701 192.168.137.203 192.168.137.1 DNS 73 Standard query 0x7103 A www.baudi.com
Standard query response 0x7103 A www.
638 18.30100 192.168.137.1 192.168.137.203 DNS 132 baidu.com CNAME www.a.shifen.com A
115.239.210.27 A 115.239.211.112
```

图 1 DNS 域名查询请求

一次域名查询的流程如图 1 所示,客户端向 DNS 服务器请求域名 www.baidu.com 的 IP 地址,之后 DNS 服务器回复

客户端 www.baidu.com 的 IP 地址为 115.239.211.112,然后客户端就可以向这个 IP 地址发起 HTTP 请求,从而实现

网站的访问。一般客户端的 DNS 地址是通过 DHCP 的方式从网关获取到的,因此只要在网关上做好配置,将自己搭建的 DNS 服务的服务器地址分配给客户端,即可控制客户端访问网页的 IP 地址。

当网关将我们自己搭建的 DNS 服务器地址分配给客户端后,客户端再次访问 www. baidu. com 时,客户端先通过搭建的 DNS 服务器查询 www. baidu. com 的 IP 地址,此时我们的 DNS 服务器以我们自己搭建的代理服务器的 IP 地址,代替百度的真实 IP 地址,回应客户端的 DNS 查询请求。如此一来,客户端就会在无感知的情况下将原本发给百度的 HTTP 请求发送给我们的代理服务器,从而可以在代理服务器上分析 HTTP 请求,达到审计客户端上网行为的目的^[3]。与此同时,为了保证客户端正常的上网功能不受任何影响,还需对代理服务器做特殊的配置。

1.2 HTTP 透明代理

代理服务是一种特殊的网络服务,这种服务允许一个客户端通过代理服务与一个服务器进行非直接连接。提供代理服务的电脑系统或其它类型的网络终端称为代理服务器(Proxy Server)。一个完整的代理请求过程为:客户端首先与代理服务器创建连接,接着根据代理服务器所使用的代理协议,请求对目标服务器创建连接或者获得目标服务器的指定资源。在后一种情况中,代理服务器可以下载目标服务器的资源至本地缓存,如果客户端所要获取的资源在代理服务器的缓存之中,则代理服务器便不会向目标服务器再次发送请求,而是直接返回缓存的资源^[4]。因此代理服务有利于保障网络终端的隐私和安全,同时也有助于提高客户端网络访问的速度。

由于普通的代理服务器需要在客户端的浏览器上进行设置才能发挥代理作用,而本文所设计的网络安全审计系统是在用户无感的状态下进行安全审计的,因此需要一种无需客户端设置的代理模式,即通过透明代理来实现。透明代理是一种客户端感觉不到代理服务存在的代理模式,无需在客户端上做任何设置,客户端所有的访问数据会自动被重定向到代理服务器的代理端口,再由代理服务器向英特网请求所需的数据并转发给客户端^[5]。

当客户端通过 DNS 解析,将其 HTTP 请求发送到我们代理服务器的 IP 时,我们的代理服务器向客户端真正要访问的服务器转发客户端的 HTTP 请求,再将真正要访问的服务器返回过来的数据转发给客户端,由此保证客户端的网络访问得以成功,最终实现一个功能完整的网络安全审计系统,如图 2 所示。

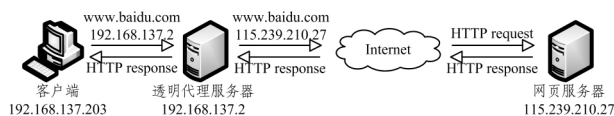


图 2 DNS 重定向系统网络结构

1.3 ACL 访问控制

在网络安全审计系统中,可以通过访问控制列表(AccessControlList, ACL)对数据包进行过滤,从而有效地防止违法用户或用户对违规网站的访问。ACL 的原理是先获取路由需要转发的数据包的包头信息,然后与设定的规则进行比较,规则可以是数据包的源地址、目的地址、端口、协议类型或

关键字等,ACL 会根据比较的结果对数据包进行转发或者丢弃^[6]。

访问控制列表不但可以起到控制网络流量、流向的功能,而且在很大程度上起到保护网络设备、服务器的关键作用。在网络安全审计系统中加入 ACL 访问控制,可以将被动的网络安全审计提升为主动的安全防御,从而成为保护内网安全的有效手段。

ACL 访问控制列表的工作流程如图 3 所示,当数据流进入方向的接口收到一个分组时,系统会检查其路由,如果是不可路由,则会直接丢弃;如果是可路由,则判断接口是否配置了 ACL。如果没有配置,则直接查询路由表,然后根据路由表中找到的端口准备往外转发;如果配置了 ACL,系统则检查 ACL 规则是否允许该分组通过,不允许则丢弃,允许则查询路由表,选择外出接口准备往外转发。当外出接口选择好之后,系统再次检查外出接口是否配置 ACL,如果配置了 ACL,则检查 ACL 指令组是否允许;若没有配置 ACL,则直接转发^[7]。

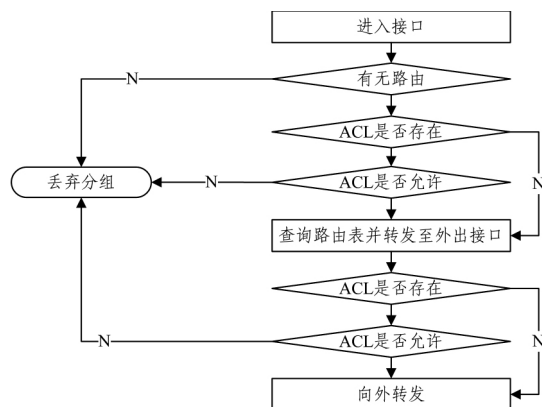


图 3 访问控制列表工作流程

2 系统实现方法

2.1 技术方案

软件列表如表 1 所列。

表 1 软件列表

操作系统	Ubuntu 14.04-desktop
DNS 服务	Bind 9.9.5
代理服务	Squid 3.1.10
审计服务	Wireshark 1.10.6

2.2 DNS 服务配置

本系统通过开源软件 Bind9 来实现 DNS 的解析功能。BIND (Berkeley Internet Name Domain) 是 DNS 协议的一个实现方式,提供了 DNS 的主要功能,包括域名服务器(named)、DNS 解析库函数、DNS 服务器运行调试所用的工具,是一款开放源码的 DNS 服务器软件,由美国加州大学 Berkeley 分校开发和维护。按照 ISC 的调查报告,BIND 是世界上使用最多最广泛的域名服务系统。

在 Ubuntu 系统上可以通过 apt-get 命令直接获取该软件。安装完 Bind9 后,需要修改位于/etc/bind 目录下的 named.conf.local 配置文件,在其中以如下格式添加顶级域名支持列表(以 .com 域名为例):

```
zone "com" {
    type master;
```

```
file "db.com";
};

    添加完成后,继续在/var/cache/bind 目录下新建名为
    “db.com”的配置文件,并以如下格式配置域名解析地址:
    $TTL 604800
    @ IN SOA com. root. com. (
        20;Serial
        604800;Refresh
        86400;Retry
        2419200;Expire
        604800);Negative Cache TTL
    ;
    @ IN NS localhost.
    *.com. IN A 192.168.137.2
```

在经过上述配置后,当客户端访问以.com 域名为域名结尾的服务器时,该 DNS 服务器皆会回应该域名的 IP 地址为 192.168.137.2,之后客户端就会将所有 HTTP 请求都发往 192.168.137.2 这个内网的 IP 地址,由此实现了客户端数据的初步重定向。

2.3 代理服务配置

本系统的透明代理功能是通过开源软件 Squid 实现的。Squid cache (简称为 Squid) 是一个流行的代理服务器和 Web 缓存服务器软件(GNU 通用公共许可证)。Squid 有广泛的用途,作为网页服务器的前置,cache 服务器可以缓存相关请求来提高 Web 服务器的速度,为代理客户端共享网络资源、域名系统和其他网络搜索,也可以通过过滤流量来提高网络安全。Squid 主要运行于 Unix 一类系统,具有相当悠久的历史,功能也相当完善。除了 HTTP 外,对于 FTP 与 HTTPS 的支持也相当好,同时也支持 IPv6。

编译并安装好 Squid 后,修改位于/usr/local/squid/etc/目录下的 squid.conf 配置文件,将如下两行配置添加至该配置文件:

```
http_access allow all
http_port 192.168.137.2:3128 transparent
```

上述配置表示允许 HTTP 请求通过代理服务器,经 192.168.137.2 的 3128 端口进行透明转发。代理服务设置完成后,还需开启 Linux 系统的 iptables 数据转发,在命令行中依次输入如下命令:

```
echo 1>/proc/sys/net/ipv4/ip_forward
iptables-t nat-A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 3128
```

```
iptables-t nat-A POSTROUTING -o eth0 -MASQUERADE
```

上述命令首先开启了 Linux 的 IP 转发功能,然后将 80 端口接收到的 tcp 协议全部转发到 3128 端口,再以 Linux 系统中 eth0 为出口对外访问英特网。至此所有配置完成,该网络安全审计系统已可以上线运行。

2.4 审计服务配置

本系统的审计服务是通过 Wireshark 软件来演示的。Wireshark 是一种网络封包分析软件,功能是抓取网络封包,并尽可能显示出最为详细的网络封包信息。它虽然不是专业的审计软件,其对网络上的异常流量行为不会产生警示或是任何提示,但通过仔细分析 Wireshark 抓取的封包,能够帮助网络管理员更清楚地了解网络中发生的行为。

在按上文步骤搭建完 DNS 和透明代理服务器后,局域网中所有的上网数据都会经过透明代理服务器的 eth0 接口进行转发,因此只要在该服务器上安装 Wireshark 软件,运行并监听 eth0 上的数据,即可显示出当前网络中所有的流量信息。当审计到网络中的非法行为需要对某些客户端进行限制时,可以在 Squid 服务的配置中加入 ACL 访问控制列表,对特定地址或访问行为进行允许或拒绝通过的措施。如果网络管理员有专业的网络审计软件,也可以通过监听 eth0 接口的方式,对全网的数据流量进行专业审计。

2.5 访问控制列表配置

本系统是通过 Squid 代理服务实现 ACL 访问控制功能的。在 squid.conf 文件中,加入 acl 语句即可实现访问控制,语法为 acl aclname [acltype [string1]],其中 acltype 的类型如表 2 所列。

表 2 acltype 规则类型

src	源地址
dst	目的地址
sredomain	客户域
dstdomain	服务域
url_regex	URL 规则表达式匹配
urllpath_regex	URL-path 规则表达式匹配
time	访问时间
port	访问端口
proto	传输协议
method	请求方法

例如,要禁止内网 IP 为 192.168.137.203 的用户访问优酷网时,即可编写如下 3 条语句加入配置文件中^[8]:

```
acl client src 192.168.137.203
acl client_url url_regex ^http://www.youku.com
http_access deny client client_url
```

访问控制列表启动后,当 IP 为 192.168.137.203 的客户端自动通过代理服务访问优酷时,该请求就会被代理服务直接丢弃,从而达到禁止特定客户端访问特定网站的效果。

3 系统测试

由于 DHCP 协议本身就存在服务器与客户端之间双向认证的安全性问题,导致在进行 DHCP 协议交互时,客户机无法实现对服务器的认证^[8]。

在作为网关的路由器中,找到 DHCP 配置,修改其中的 DNS 服务器为 192.168.137.2,如图 4 所示。



图 4 通过 DHCP 修改 DNS 服务器

重启路由器后,在客户端上使用 ping 工具解析 www.sina.com 域名,获得来自 192.168.137.2 的回应,如图 5 所示,表明 DNS 重定向已生效。

```
D:\>ping www.sina.com
```

正在 Ping www.sina.com [192.168.137.2] 具有 32 字节的数据:

来自 192.168.137.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.137.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.137.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.137.2 的回复: 字节=32 时间<1ms TTL=64
192.168.137.2 的 Ping 统计信息:
数据包: 已发送=4, 已接收=4, 丢失=0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短=0ms, 最长=0ms, 平均=0ms

图 5 DNS 重定向效果

客户端打开浏览器访问 www.sina.com 网站, 成功显示了网站的所有内容, 同时在网络安全审计系统上使用 Wireshark 软件分析 eth0 接口上的数据流量, 即可得到如图 6 所示的信息。

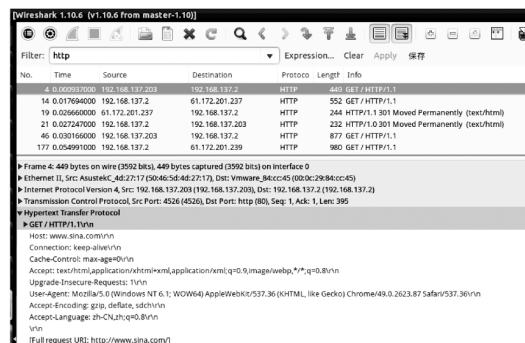


图 6 审计系统工作效果

从图 6 的信息可以看出, 客户端 192.168.137.203 首先向审计服务器 192.168.137.2 发送了访问 www.sina.com 的 HTTP 请求, 由此审计系统即审计了客户端的访问记录, 之后审计系统向真正的网页服务器 61.172.201.237 转发了客户端的 HTTP 请求, 并在得到网页服务器的回应后, 将回应内容转发回客户端, 由此保证了客户端的正常上网功能不受

任何影响。而当客户端访问了被 ACL 禁止的网站时, 由于代理服务的阻止, 无法得到有效的响应, 从而使客户端无法对该网站进行访问。

结束语 本文通过多种开源软件的结合使用, 设计了一种低成本的网络安全审计系统方案, 无需在客户端上做任何改动, 只需修改网关的 DNS 设置, 即可对整个局域网内的网络访问行为进行安全审计, 非常适合小型网络管理员使用。未来还可以在该系统构架的基础上, 开发相应的分析及管理系统, 从而形成一个具有一定商业价值的网络安全审计方案, 发挥其更高的实用意义。

参考文献

- [1] 吴承荣, 廖健, 张世永. 网络安全审计系统的设计和实现[J]. 计算机工程, 1999, 25(S1): 171-174
- [2] 吴琼. DNS 服务应用于局域网教学的研究[J]. 吉林工程技术师范学院学报, 2010, 26(1): 77-80
- [3] 胡小梅, 刘嘉勇. 基于 DNS 劫持的流量监测系统设计与实现[J]. 网络安全技术与应用, 2016(1): 110-112
- [4] 百度百科. 代理服务器[EB/OL]. (2014-06-30) [2016-04-21]. [http://baike.baidu.com/link?url=8R7SISgG8VHHdLyWje5aPu2EM7kFABwodaXOkN9mKw2F2DIUNrmuMED7tqpt9cE2QFRnigfv8ZV33Kd1V094Bq#reference-\[1\]-751-wrap](http://baike.baidu.com/link?url=8R7SISgG8VHHdLyWje5aPu2EM7kFABwodaXOkN9mKw2F2DIUNrmuMED7tqpt9cE2QFRnigfv8ZV33Kd1V094Bq#reference-[1]-751-wrap)
- [5] 何文华, 梁竞敏. Linux 下传统代理、IP 伪装与透明代理的设计与实现[J]. 计算机系统应用, 2004(10): 60-62
- [6] 诸晔. 用 ACL 实现系统的安全访问控制[J]. 计算机应用与软件, 2005, 22(03): 111-114
- [7] 晴刃. 访问控制列表(ACL)实例详解[EB/OL]. (2012-11-25) [2016-05-09]. <http://www.qingsword.com/qing/696.html>
- [8] 何博远. 局域网环境下利用 DHCP 欺骗技术实现 DNS 劫持攻击[J]. 现代计算机(专业版), 2011(14): 44-47
- [9] Mederos B, Amenta N, Velho L, et al. Surface Reconstruction from Noisy Point Clouds[C] // Proceedings of the third Eurographics Symposium on Geometry Processing (SGP2005). Vienna, Austria, 2005: 53-62
- [10] 董辰世, 汪国昭. 一个利用法矢的散乱点三角剖分算法[J]. 计算机学报, 2005, 28(6): 1000-1005
- [11] Carr J C, Beatson R K, Cherrie J B, et al. Reconstruction and representation of 3D objects with radial basis functions[C] // Proceedings of the 28th Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH 2001). ACM Press, 2001: 67-76
- [12] Alexa M, Behr J, Cohen-Or D, et al. Computing and rendering point set surfaces[J]. IEEE Transactions on Visualization and Computer Graphics, 2003, 9(1): 3-15
- [13] Du H, Qin H. A shape design system using volumetric implicit PDEs[J]. Computer-Aided Design, 2004, 36(11): 1101-1116
- [14] Ohtake Y, Belyaev A, ALEXA M, et al. Multi-level partition of unity implicits[J]. Proceedings of ACM SIGGRAPH 2003, ACM Press, San Diego, USA, 2003, 22(3): 463-470
- [15] Kazhdan M, Bolitho M, Hoppe H. Poisson surface reconstruction[C] // Proceedings of the Fourth Eurographics Symposium on Geometry Processing, Sardinia, Italy, 2006: 61-70
- [16] Bernardini F, Mittleman J, Rushmeier H, et al. The ball-pivoting algorithm for surface reconstruction[J]. IEEE Transactions on Visualization and Computer Graphics, 1999, 5(4): 349-359
- [17] Kuo C C, Yau H T. A Delaunay-based region-growing approach to surface reconstruction from unorganized points[J]. Computer-Aided Design, 2005, 37(8): 825-835
- [18] Kuo C C, Yau H T. A new combinatorial approach to surface reconstruction with sharp features[J]. IEEE Transactions on Visualization and Computer Graphics, 2006, 12(1): 73-82
- [19] 方林聪, 汪国昭. 基于径向基函数的曲面重建算法[J]. 浙江大学学报(工学版), 2010, 44(4): 728-731
- [20] 赵建东, 康宝生, 康健超, 等. 改进的基于径向基函数的曲面重建算法[J]. 西北大学学报(自然科学版), 2012, 42(5): 744-748
- [21] 钱归平, 童若锋, 彭文, 等. 基于散乱点云内部特征的网格重建[J]. 浙江大学学报(工学版), 2008, 42(5): 732-735
- [22] 聂建辉, 马孜, 胡英, 等. 针对密集点云的快速曲面重建算法[J]. 计算机辅助设计与图形学学报, 2012, 24(5): 575-582
- [23] Huang H, Li D, Zhang H, et al. Consolidation of unorganized point clouds for surface reconstruction[J]. ACM Transactions on Graphics, 2009, 28(5): 1-7
- [24] Huang H, Wu S, Gong M, et al. Edge-aware point set resampling[J]. ACM Transactions on Graphics, 2013, 32(1): 1-12