基于网络文本信息隐藏技术的研究 *

杨 杰，卢选民，张辉栋，李成福
（西北工业大学 电子信息学院，陕西 西安 710129）

摘 要： 信息隐藏是网络时代信息安全领域新兴起的一个研究热点。基于 Netfilter/iptables 模块和 MITM(Man-in-the-Middle)技术，在 Linux 环境下通过 L7-filter 和 Ettercap 技术实现了 NAT 服务器对流入内部网络的不良文本信息的隐藏和替换。通过网络实验证明，达到了预期的设计目的。

关键词： Netfilter/iptables；MITM；L7-filter；Ettercap；信息隐藏与替换
中图分类号： TP309 **文献标识码：** A **文章编号：** 1674-7720(2013)08-0010-03

Research on network text information hiding technology

Yang Jie, Lu Xuanmin, Zhang Huidong, Li Chengfu
(School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710129, China)

Abstract: Information hiding has become a new hot interest area in the research of information seeurity in the network age. In this paper, hiding and replacing the bad text information flowing to the internal network of NAT server are implemented based on Netfilter/iptables modules and the Ettercap technique in Linux OS. The experiment shows that it achieves the desired results.

Key words: Netfilter/iptables; MITM; L7-filter; Ettercap; information hiding and replacement

随着 Internet 的迅速发展，信息隐藏成为网络时代信息安全领域兴起的一个研究热点，在版权保护、隐蔽通信等许多方面有着非常广阔的应用前景[1]。信息隐藏被用来保护信息安全的同时，也可能被用来传送一些不良信息给网络用户，如何过滤或者截获并替换掉这些不良信息，就成为该领域研究的热点。

针对 NAT 服务器对流入内网的不良文本信息的隐藏和替换问题(图 1 为网络拓扑图)，本文基于 Netfilter/iptables 模块和 MITM 技术，在 Linux 环境下通过 L7-filter 和 Ettercap 技术实现了网络文本信息的隐藏和替换。

1 Netfilter/iptables 模块

在 Linux 系统中，Netfilter 是其内核的一个完整且功能强大的防火墙系统；iptables 模块则是 Netfilter 提供的一种用户工具，是与 Linux 内核集成的 IP 信息包过滤系统[2]。通过这种工具可以实现 NAT，进而隐藏 IP 地址信息。

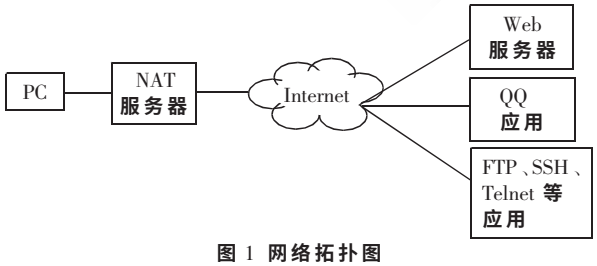

图 1 网络拓扑图

iptables 的基本语法规则如下：

iptables [-t table] command [match] [target]；

iptables 中共有三类表：Mangle、Nat 和 Filter。Mangle 表对于满足常规的防火墙应用作用不大。Nat 表的作用在于对数据包的源或目的 IP 地址进行转换[3]。Nat 表又可主要分为三条链：(1)DNAT：改变包的目的地址，以使包能从路由到某台主机上；(2)SNAT：改变包的源地址，可以隐藏用户的本地网络；(3)MASQUERADE：与 SNAT 作用基本一样，对每个匹配的包，MASQUERADE 都要查找可用的 IP 地址。Filter 表用来过滤数据包，可以在任何时候匹配并过滤包，对包做 DROP 或 ACCEPT。

iptables 模块处理流程[2]：首先，当一个包进来时，内核根据路由表决定包的目标。如果目标主机就是本机，则直接进入 INPUT 链，再由本地正在等待该包的进程接收；否则，如果进来的包的目标不是本机，则看是否内核允许转发包[4-5]。最后，Linux 防火墙主机本身能够产生

* 基金项目：2012 年西北工业大学研究生创业种子基金项目(Z2012085)

包，这种包只经过 OUTPUT 链被送出防火墙。图 2 给出了数据包经过 iptables 模块的处理流程。

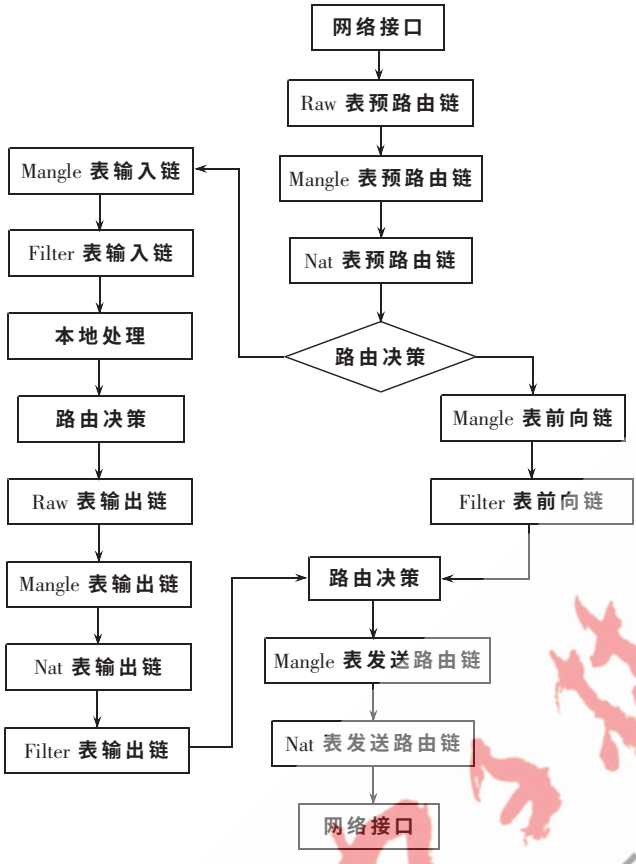

图 2 数据包经过 iptables 模块的处理流程

2 基于 L7-filter 的匹配与替换

L7-filter 是一个 Netfilter/iptables 的增强型补丁插件，它的核心是通过一个工作在内核级的可对数据包进行分类的补丁程序与 iptables 进行联动，与其他基于端口包分类工具的不同处在于，它是基于数据内容匹配和分析的[2]。利用正则表达式匹配 Layer7 应用协议(HTTP、FTP)的传输数据，能更准确地分析数据包。

L7-filter 在默认情况下，将同一个连接中的 10 个数据包或者 2 KB 的数据包内容放在缓存中。并将缓存中的内容作为一段普通的文本，用模板文件中的正则去搜索，如果发现有正则匹配的内容，就会在 Netfilter 中将这几个数据包 DROP 丢掉或者给数据包打上标记。

下面就是该命令对于数据包中的内容进行匹配及替换的命令：

```
#iptables -A FORWARD -m mark --mark 1 -m filter-string --string "xxx.xxx.xxx.xxx" --replace-string "xxx.xxx.xxx.xxx"?-j LOG --log-prefix "ip filter:"
```

3 基于 MITM 和 Ettercap 的匹配与替换

中间人攻击 MITM(Man-in-the-Middle Attack)是一种“间接”的入侵攻击，这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。然后入侵者把这台计算机模拟为一台或两台原始计算机，使“中间人”能够与原始计算机建立活动连接并允许其读取或修改传递的信息，然而两个原始计算机用户却认为他们是在互相通信。通常，这种“拦截数据——修改数据——发送数据”的过程就被称为“会话劫持”。

Ettercap 是基于 MITM 技术的一款有效的、灵活的中介工具。利用其特性可以实现数据包过滤和丢弃以及替换功能：可以建立一个查找特定字符串的过滤链，根据这个过滤链对 TCP/UDP 数据包进行过滤并用自己的数据替换这些数据包，或丢弃整个数据包。它可以支持并收集以下协议的口令信息：TELNET、FTP、POP、RLOGIN、SSH1、ICQ、SMB、MySQL、HTTP 等。通过 shell 脚本的编写可以实现基于 Ettercap 的文本内容匹配与替换。

ettercap.sh 源代码：

```
#! /bin/bash
EF=/usr/bin/etterfilter
EC=/usr/sbin/ettercap
FILTER=.stringreplace.ef
echo "Remember, Press q to qiut! "
echo "Which data in the packet do you want to change?"
read DATA1                                    //输入想替换的文本
echo "what do you want to change $DATA1 to ?"
read DATA2                                    //替换成的文本
#(echo $DATA1|wc -m)-(echo $DATA2|wc -m)
#if [((echo $DATA1|wc-m)-(echo $DATA2|wc -m))! =0]
# then
# echo "The numbers of characters of $DATA1 must be
    the same with $DATA2"
# exit
rm -rf ./change_data
mkdir ./change_data
DIR=change_data
cd $DIR
touch .stringreplace.filter
FILE=.stringreplace.filter
echo "if(ip.proto==TCP && tcp.src == 80){" > $FILE
echo """>>$FILE
echo "if (search(DATA.data, \"$DATA1\")){" >> $FILE
echo " replace(\"$DATA1\",\"$DATA2\");">> $FILE
echo "}">>$FILE
echo "}" >>$FILE
$EF $FILE -o $FILTER
$EF -t $FILTER
$EC -i eth0 -Tq -F $FILTER -M arp
echo "You have successfully quited changing $DATA1 to
    $DATA2"
```

4 实验结果及分析

通过在终端下运行 shell[3]脚本即可实现基于文本的隐藏与替换。为了方便用户操作，基于 JAVA Swing 组

图 3 文本替换的界面

件[4]编写了如图 3 所示的软件。

用户可以按要求填写内容，然后单击替换按钮后程序即可运行。当内网用户发出请求后，若响应内容中包含用户要替换的内容，NAT 服务器会将该文本替换成用户设定的，然后结果信息返回给用户，从而实现网络文本的替换。

在 Linux 操作系统下，实验结果如下：图 4 所示为替换之前的文本内容，图 5 所示为替换之后的文本内容，从而实现了网络文本的隐藏与替换功能。

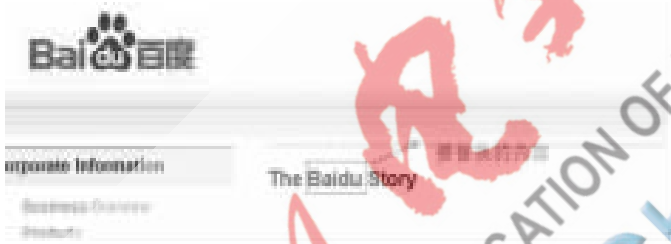

图 4 替换之前的内容

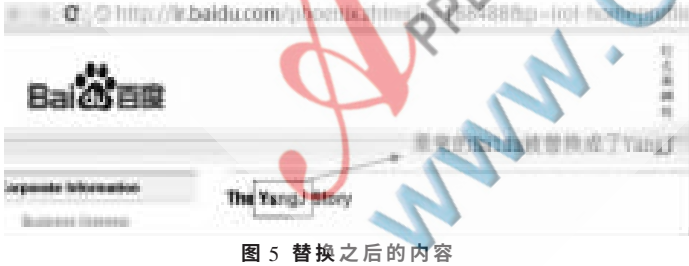

图 5 替换之后的内容

在 html 网页中，<body>标签中的文本内容基本上都可以匹配并替换成预先设定的，然而有的内容是通过脚本语言实现的，还有很多脚本文件是通过压缩文件发送到客户端的，这种的就匹配不到。

针对这种情况，可以利用 iptables 的过滤无效数据包的功能，当发现某网页中包含想要替换的文本但却替换不了时，可以将该数据包过滤掉。应用程序界面如图 6 所示。

本文针对 NAT 服务器对流入内网的不良文本信息

图 6 文本过滤界面

的隐藏和替换问题，基于 Netfilter/iptables 模块和 MITM 技术，在 Linux 环境下通过 L7-filter 和 Ettercap 技术实现了网络文本信息的隐藏和替换。同时，通过网络实验验证了其有效性。

参考文献

[1] CACHE J，WRIGHT J.黑客大曝光：无线网络安全[M]. 李瑞民，译.北京：机械工业出版社，2012.

[2] RASH M. Linux 防火墙[M]. 陈健，译. 北京：人民邮电出版社，2009.

[3] 丰士昌. Linux 指令与 Shell 编程[M].北京：科学出版社，2012.

[4] 王鹏，何昀峰. Java Swing 图形界面开发与案例详解[M]. 北京：清华大学出版社，2008.

[5] 白滔，刘大滢. Linux 下怎样利用 Iptables 实现网络防火墙的监控功能[J]. 贵州气象，2006，30(4):33-35.

[6] 郝慧珍，傅汝林.基于 IP 伪装的网络安全技术研究[J]. 成都理工学院学报，2002，29(3):315-319.

[7] Zhang Lixia. A retrospective view of network address translation[J]. IEEE Network，2008，22(5):8-12.

[8] HEAGARTY T.Using iptables and the netfilter framework [OL].(2007-03-xx)[2012-12-13]inDEPTH，www.ipmagazine.org/en：LINUX+DVD 3/2007.

[9] ANDREASSON O.Iptable tutorial[OL].http://www.frozentux.net/documents/iptables-tutorial/.

(收稿日期：2012-12-31)

作者简介：

杨杰，男，1988 年生，硕士研究生，主要研究方向：网络信息安全。

卢选民，男，1972 年生，副教授，博士后，主要研究方向：智能信息处理与计算机网络等。