UDP 反射 DDoS 攻击的原理和防范

李刚，丁伟

(东南大学计算机科学与工程学院，江苏南京 211189)

摘要：UDP 反射 DDoS 攻击（即 DrDoS 攻击）是一类利用网络协议漏洞发动的 DDoS 攻击，这种攻击的流量放大效果能够对被攻击者造成较大影响。结合网络管理平台 NBOS 检测出的反射攻击和其他相关文献，本文介绍了反射 DDoS 的原理，讨论了被利用进行攻击的协议漏洞，并就这些协议的攻击防范在主机服务设置方面提供了参考意见。

关键词：反射 DDoS 攻击；协议漏洞；攻击防范

1 引言

2013 年 5 月，国家互联网应急中心(CNCERT)发布的《2013 年中国互联网网络安全报告》称，DDoS 攻击依然是我国互联网基础设施和信息系统正常运转的主要威胁，且呈现日益严重的趋势，其中反射放大攻击逐渐增多，且规模巨大[1]。2013 年 3 月，国际反垃圾邮件组织 Spamhaus 遭受攻击，攻击者借助现网开放的 DNS 群，利用 DNS 反射技术，将攻击流量轻松放大约 100 倍，峰值达 300Gbit/s；2014 年初，黑客利用时间同步服务 NTP 对 EA 等大型游戏网站发动 DDoS 攻击；美国 CDN 服务商 CloudFlare 亦声称遭受过高达 400Gbit/s 流量的 NTP 反射攻击。

2013 年以来，反射攻击的报道层出不穷。相对于传统的基于僵尸网络的 DDOS 攻击，由于反射放大攻击不需要僵尸进程的帮助，因此实现和控制过程相对简单，因此成本较低，且具有放大效果显著、追溯困难的特点。这给传统的 DDoS 攻击的防护带来新的挑战。本文将对反射攻击的原理进行分析，讨论主流攻击协议的主要漏洞，并给出相应的防范提建议。

2 反射 DDoS 攻击的原理

分布式拒绝服务(DDoS:Distributed Denial of Service)攻击是指利用足够数量的傀儡计算机产生数量巨大的攻击数据包，对网络上的一台或多台目标实施 DoS 攻击，从而耗尽受害目标的资源，迫使目标失去提供正常服务的能力[2]。

基于 UDP 报文的反射 DDoS 攻击是这类攻击的一种实现形式。攻击者不是直接发起对攻击目标的攻击，而是利用互联网的某些服务开放的服务器，通过伪造被攻击者的地址、向有该服务器发送基于 UDP 服务的特殊请求报文，数倍于请求报文的回复的数据被发送到被攻击 IP，从而对后者间接形成 DDOS 攻击。图 1 是这类攻击的一个攻击场景。

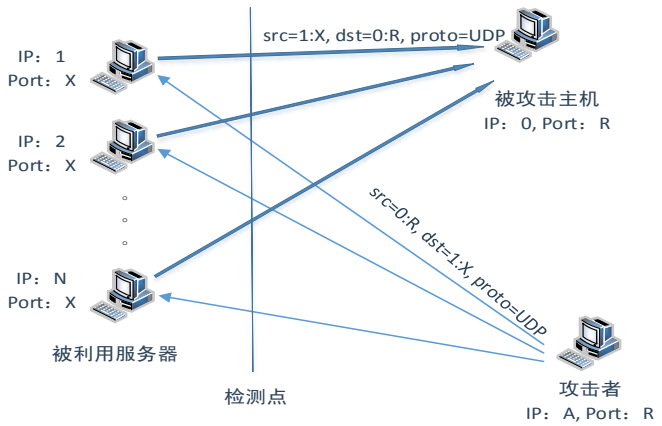

图 1UDP DRDDOS 攻击场景

简单来讲，这类攻击是基于无连接的 UDP 协议设计的网络服务的设计"缺陷"和目前 IP 网不做真实原地址检查这个条件设计的。攻击者通过扫描，确认服务的开放和漏洞的存在后，即可对这些服务器发送请求，通过伪造源地址的方式对特定目标发动反射攻击。

3 反射攻击的协议漏洞分析

2014 年德国波鸿大学的一篇研究报告对 14 种 UDP 协议进行了系统的实验性研究[3]，认为这些协议存在实施反射攻击的可能，并提出了协议的“带宽放大因子（BAF, Bandwidth Amplification Factor）”的概念，即回复报文的总字节数与请求报文字节数的比值。显然，服务协议的 BAF、攻击脚本实现的便捷性是攻击者选择协议进行攻击是的主要考虑因素。

来自 Arbor、AT&T 等设备厂商的近期报道[4][5]中，上述 14 中协议中的 5 种在当前的网络环境中是可见的，分别是 Chargen、SNMP、DNS、NTP 和 SSDP。

由于不同版本的实现机制各不相同，加上对请求数据支持的多样性，同一服务的 BAF 值也会存有一定的差异。我们根据文献[6-11]构造请求报文，利用试验室环境和 CERNET 中有反射攻击行为的主机进行了实验，得到了“实验 BAF”。文献[3]也给出了作者自己的试验结果，以下称为“标准平均 BAF”。协议漏洞、实验 BAF 和标准平均 BAF 的具体情况是：

- Chargen（字符发生器协议）

Chargen 协议的设计中规定每当服务器收到一个 UDP 数据包后向客户端返回一个数据包，其中包含长度为 0~512 字节之间随机值的任意字符。这个协议在 Linux 系统和 windows 系统中的实现有所不同，实验 BAF 约为 15-50。标准平均 BAF：358.8。

- NTP（Network Time Protocol，网络时间协议）

NTP 早期版本中的 monlist 请求功能支持客户端使用一次请求最多可获取 600 个与服务器同步的客户 IP 地址，这些地址信息还被分到多个数据包中进行回复。试验 BAF 为 200 左右，标准平均 BAF 是 556.9。

- DNS（Domain Name System，域名系统）

产生的原因是开放 DNS 服务器对 dig 查询的支持，将 OPT RR 字段中的 UDP 报文大小设置较大的数值（如 4096），一般 60 字节的查询可以获得 3000 字节的返回数据包，实验 BAF 值为 50。标准平均 BAF：28.7~54.6。

- SSDP（Simple Sever Discovery Protocol，简单服务发现协议）

设置 SSDP 报头的 ST 字段为“all”，即所有设备和服务。在实验环境下，一个 135 字节的请求报文获得了 10 个 350 字节报文的回复，即试验 BAF 为 25。标准平均 BAF：30.8。

- SNMP（Simple Network Management Protocol，简单网络管理协议）

SNMPv2 版中引入的 snmpbulkget 功能支持用单个请求报文获得管理数据，试验中一个 1350 字节的请求报文获了得 20 个 1500 字节的回复，实验 BAF 为 20。标准平均 BAF：6.3。

4 反射攻击的防范措施

上述协议安装后由于有关服务默认处于开启状态，是其被利用的一个重要因素。因此，防范可以从配置主机服务选项和访问控制权限（ACL）入手。具体建议如下：

- Chargen 攻击防范配置方法

关闭 Chargen 服务，具体的操作方法：

a) Linux 系统：在/etc/inetd.conf 文件中注释掉'chargen' 服务，或者在/etc/xinetd.d/ 目录下将 chargen 服务对应的文件中的"disable" 属性改为 "yes"。

b) 在 Window 系统下：Chargen 服务属于 Windows 系统中的 SimpTCP 服务，一般情况下 Windows 系统缺省不会安装该服务，如已安装该服务，可以通过如下几种方式关闭服务：
1) 通过控制面板中的 Service 管理程序，关闭 SimpTCP 服务；

2) 通过修改注册表：通过注册表编辑器将以下两项表项的值设为 0

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen

3) 通过命令行执行 net 程序：net stop simptcp；net start simptcp。

- NTP 攻击防范配置方法

1.升级版本

Linux 系统中的 ntpd 4.2.7p26 及之后的版本关闭了 monlist 请求功能。升级到 ntpd 4.2.7p26 或更高版本可以避免针对该漏洞的攻击。

2. 禁用或限制状态查询

a) 在 Linux 系统下，如果 monlist 功能开放，可尝试通过修改 ntp.conf 配置文件解决问题，具体操作建议是在上述文件中增加下面的配置：

IPV4: restrict default kodnomodifynotrapnopeernoquery

IPv6: restrict -6 default kodnomodifynotrapnopeernoquery

另外，还可以配置限制访问命令，如：restrict default noquery。

b) Windows Server 系统的设置方法较为简单：在 ntp.conf 配置文件中增加（或修改）“disable monitor”选项，可以关闭现有 NTP 服务的 monlist 功能。

修改并保存配置文件之后，请重启 ntpd 服务。

- DNS 攻击防范配置方法

1. 关闭递归查询

a) 在 UNIX 系统的 DNS 服务器下：在全局配置选项中加入如下限制以关闭递归查询：

options {allow-query-cache { none; }; recursion no;};

b) 在 Windows 系统的 DNS 服务器下，采取如下步骤：(1) 打开 DNS（“开始”-“程序”-“管理工具” -单击“DNS”）；(2) 在控制列表树中，单击“适用的 DNS 服务器”；(3) 在“操作”菜单上，单击“属性”；(4) 点击“高级”；(5) 在“服务器选项”中，选中“禁用递归”复选框，然后确定。

2. 授权特定用户进行递归查询

在特定组织或者 ISP 中部署的 DNS 服务器，域名解析应当配置成对授权的客户机提供递归查询。这些递归查询请求应当只来源于该组织内的客户机地址。建议所有的服务器管理员只允许内部客户机的递归查询请求。

在 UNIX 系统的 DNS 服务器配置下，在全局配置选项中做如下设置：

acl corpnets { 192.168.1.0/24; 192.168.2.0/24; };

options {allow-query { any; };allow-recursion { corpnets; };};

- SSDP 攻击防范配置方法

1. 关闭系统服务

a)在 Windows 下以管理员身份运行 cmd.exe，并执行以下命令：scconfig SSDPSRV start= DISABLED；b)在桌面上右击“计算机”，在“服务和应用程序”中点击“服务”，找到“SSDP Discovery”服务，双击后该服务后选择“禁用”选项。

2. 防火墙拦截

a) 在 Windows 系统操作如下：

在“开始”-“控制面板”-“Windows 防火墙”-“高级设置”中，分别在“入站规则”和“出站规则”中加入一条新的规则，新建规则操作如下：点击“新建规则”，选择“端口”和“下一步”，选择“UDP”，并在“特定远程端口中”输入“1900”，点击“下一步”，选择“阻止连接”和“下一步”，选择“域”、“专业（P）”、“公用（U）”和“下一步”，在名称中输入“SSDP Discovery”，并点击“完成”。

b) 在 Linux 系统操作如下：

（1）打开/etc/sysconfig/iptables 文件（操作以 CENTOS 为例），在文件中加入如下规则：

-A INPUT -p udp -m udp --sport 1900 -j DROP

-A INPUT -p udp -m udp --dport 1900 -j DROP

-A OUTPUT -p udp -m udp --sport 1900 -j DROP

-A OUTPUT -p udp -m udp --dport 1900 -j DROP

（2）最后重启防火墙：#service iptables restart

需要另外说明的是，Chargen、NTP、DNS 协议也可以在路由器或防火墙配置过滤条件，拦截目的或者源端口为相应服务端口（19 号、123 号、53 号端口等）的所有 UDP 报文，配置规则可参考上述 1900 端口的规则格式。

- SNMP 攻击防范配置方法

SNMP 服务通常用于远程监控网络设备状态，例如路由器、交互机、网络打印机、以及其它联网的嵌入式设备，不同类似的设备 SNMP 服务配置方式存在差异，有些具备 ACL 功能，有些缺少相应的访问控制。因此通用的解决方法是在边界防火墙上拦截目的或者源端口为 161 的 UDP 报文，具体方式和 SSDP 等类似。

本文针对主机服务配置的防范讨论大致如上。限于篇幅，针对单个协议的防护技术（如应用于 DNS 反射攻击防范的 Anycast 流清洗技术[13]）等相关内容不再详细列出。

5 小结

本文分析了反射 DDoS 攻击的原理、攻击特点和常见的攻击协议，包括 Chargen、NTP、DNS、SNMP 和 SSDP 协议，并对攻击相关协议的漏洞进行了详细描述。协议本身的设计缺陷以及配置不当是造成攻击的主要原因。文章最后从不同角度提出了应对该类攻击的防范措施。虽然不能从根本上杜绝攻击的发生，但是强化网络管理的意识和对设备的有效配置可以在一定程度上降低发生反射攻击的可能。

参考文献

[1] http://www.cert.org.cn/publish/main/upload/File/2013%20Annual%20Report%20.pdf

[2]李俐颖. 分布式拒绝服务攻击检测技术研究[D].电子科技大学, 2007.

[3] M Kührer,THupperich, C Rossow, T Holz. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. USENIX Security Symposium, 2014 - usenix.org.

[4] http://www.freebuf.com/news/46514.html

[5] http://techchannel.att.com/play-video.cfm/2014/8/6/

[6] Postel J. Character Generator Protocol, IETF RFC 864, May, 1983

[7] D.L. Mills. Network Time Protocol, IETF RFC 958, September 1985

[8] P. Mockapetris. DOMAIN NAMES, IETF RFC 1034, November 1987

[9] P. Vixie.Extension Mechanisms for DNS (EDNS0), IETF RFC 2671, August 1999

[10] J. Case, K. McCloghrie. Protocol Operations for SNMPv2, IETF RFC 1905, January 1996

[11] Yaron Y. Goland, Ting Cai, Paul Leach. Simple Service Discovery Protocol, IETF INTERNET-DRAFT,April 2000

[12]张阳,赵燕杰. DDoS 放大攻击原理及防护[J]. 现代计算机(专业版),2014,25:45-48.

[13]华山.基于 Anycast 架构 DNS 进行流量清洗部署方案的演进分析[J]. 电信技术, 2013, 08