TCP 反射放大攻击调研报告

一． 攻击原理

反射放大攻击是 DDoS 攻击的一种常用方式，攻击者利用网络中的放大器，将攻击流量进行放大，从而能够利用较小的带宽发起较大流量的攻击，以 DNS 反射放大攻击为例，下图是攻击示意图。

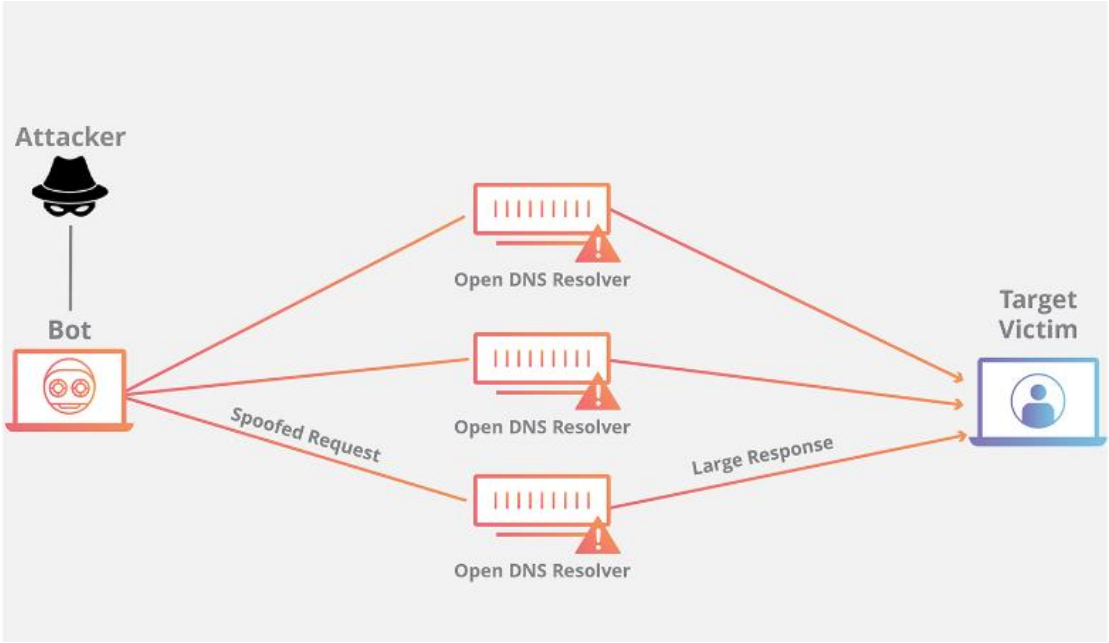

图 1 DNS 反射放大攻击示意图

在上图中，攻击者利用公开 DNS 解析器作为放大器，向放大器发送源 IP 地址为被攻击者的 DNS 请求，产生的放大后的 DNS 响应被发送给被攻击者，占用其资源造成瘫痪。在反射放大攻击的两个重要元素反射和放大中，反射通过仿冒 IP 来实现，所以这种攻击方式利用的协议通常为如 UDP 等无连接的协议，放大通过请求和响应的大小差异来实现，请求产生的响应相比请求越大，则攻击效果越好。

TCP 协议是一种有连接协议，在进行正常通讯前双方需要通过三次握手来建立连接，在连接建立过程中需要交换数据包，也即验证了用户的真实性，所以利用 TCP 进行反射放大攻击的机会只有在连接完全建立之前。TCP 反射放大攻击利用了 TCP 握手的过程，攻击者伪造源 IP 为受害者的 SYN 报文，网络中提供 TCP 应用服务的主机作为放大器，放大器接收到伪造的 SYN 请求建立连接报文后向受害者发送 SYN/ACK 响应，从而实现反射攻击。由于受害者并未向放大器发起建立连接请求，其对于接收到的 SYN/ACK 报文不会返回

ACK，放大器未接收到相应的 ACK 响应，会对 SYN/ACK 报文进行重传，通过这种方式，由一个伪造的 SYN 报文产生了多个 SYN/ACK 攻击报文，实现了放大效果。

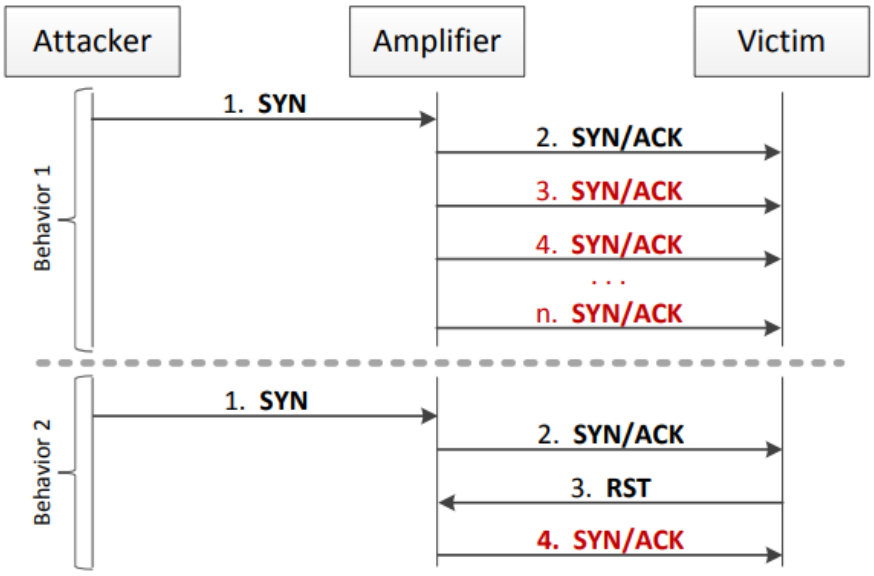

图 2 TCP 反射放大示意图

上图为 TCP 反射放大攻击的示意图，被攻击者收到 SYN/ACK 报文时有两种可能的应对方式，方式一是直接丢弃，此时放大器会尽可能的重发报文，方式二是返回一个 RST 报文来强制断开 TCP 连接，放大器仍然有可能继续发送 SYN/ACK 报文。

对于攻击者来说，相比一些不常用的协议，如 CharGen， QOTD，SSDP 等，TCP 流量不容易被拦截和过滤；另外，在 TCP 反射放大攻击中使用的是 SYN 报文，这样的报文很短并且与正常报文非常相似，从流量中检测攻击非常困难，对于其他一些反射放大攻击，通过对报文内容进行分析，攻击流量可能被检测和过滤。

TCP 反射放大攻击和 SYN 洪水攻击在方式上非常相似，区别是 SYN 洪水攻击中没有反射环节，攻击对象就是 SYN 报文发送的目标，并且 SYN 洪水攻击目的是为了耗尽被攻击方的端口资源使其无法提供服务，而反射放大攻击目的是耗尽目标的带宽及系统资源。但值得注意的是，由于 TCP 反射放大攻击和 SYN 洪水攻击在方式上类似，大规模的 TCP 反射放大攻击也可能引起连带损害，造成放大器端口资源耗尽无法提供服务。

二． 研究现状

在论文[1]中作者对 TCP 反射放大攻击进行了研究，主要关注在放大器探测，放大类型，放大性能三个方面。首先，论文中对 IPv4 空间进行探测来获取网络中潜在 TCP 反射放

大器的数量，总共收集到 480 万个独立的 IP，这些 IP 上的主机收到攻击者发送的 SYN 报文时能够向被攻击者产生 20 倍以上的攻击流量，针对不同协议的放大器探测结果如下图。

		# Amplifiers with amplification factor					
Protocol	# Responsive	> 20	> 50	> 100	> 500	> 1,000	> 2,500
FTP	152,026,322	2,913,353	3,500	1,868	1,032	937	847
HTTP	149,521,309	427,370	15,426	6,687	1,596	649	347
NetBIOS	82,706,193	12,244	2,449	1,463	873	811	783
SIP	154,030,015	22,830	5,158	3,913	3,289	3,123	2,889
SSH	141,858,473	87,715	4,611	2,141	1,275	1,176	1,082
Telnet	126,133,112	2,120,175	16,469	7,147	2,008	1,393	994

图 3 TCP 反射放大器探测结果

在对以上潜在放大器的流量分析中，以 TCP 标志位区分，放大后的流量由三种不同类型的报文组成，作者根据这一特征将放大器分为了三类并分别进行了研究。第一种放大器在连接建立失败后会继续发送 SYN/ACK 报文，试图再次建立连接，绝大多数的放大器产生的放大流量都是这种 TCP 标志位的报文，这类放大器的平均放大系数为 80 左右；第二种放大器在 TCP 连接建立失败后，会在未完成连接的状态下传输 TCP 载荷报文，这些报文的 TCP 标志位 PSH，这样的放大器数量较少，但是平均的放大系数相比响应 SYN/ACK 报文的放大器更大；第三种放大器在连接失败后会发送大量 TCP 标志位为 RST 的报文，这种类型的放大器具有极大的放大系数，最高的放大系数达到了 79625,。尽管这类放大器的数量不多，但由于极大的放大系数，在探测时这类放大器产生的攻击流量甚至远大于使用相同协议的第一类放大器。具体的放大器类型比较结果如下图。

	SYN/ACK		PSH		RST	
Protocol	# Ampl.	AF	# Ampl.	AF	# Ampl.	AF
FTP	2,907,279	22x	274	103x	5,577	53,927x
HTTP	421,487	60x	241	147x	3,411	432x
NetBIOS	8,863	54x	64	71x	3,087	78,042x
SIP	16,496	1,596x	2	696x	6,306	32,411x
SSH	81,256	80x	391	57x	5,889	29,705x
Telnet	2,112,706	28x	2,353	3,272x	4,242	79,625x

图 4 放大器按类型分类结果

由于 TCP 反射放大攻击方式中放大效果主要依赖于 TCP 对报文的多次重传，除了报文的数量之外，报文传输的频率非常重要，实际情况中同时发送报文数量才决定了放大攻击

的效果。论文中也针对攻击频率进行了测试，分别统计放大器在 10s，30s，60s 的时间内发出的报文数量，测试结果表明 SYN/ACK 和 PSH 类型的放大器攻击频率较低，RST 类型放大器的攻击频率较高。在之前的结果中 RST 类型放大器的放大系数也是三种中最高的，利用该种类型的放大器进行反射放大攻击应该能够达到比较好的效果。详细的结果如下图。

	SYN/ACK			PSH			RST		
Protocol	< 10	< 30	< 60	< 10	< 30	< 60	< 10	< 30	< 60
FTP	2	5	10	5	10	14	561	1,584	3,055
HTTP	2	6	11	5	10	16	140	224	264
NetBIOS	8	17	22	5	6	8	976	2,748	5,291
SIP	2	6	12	1	1	1	562	1,360	2,497
SSH	3	6	11	6	9	10	595	1,394	2,523
Telnet	2	5	10	52	154	277	996	2,345	4,254

图 5 放大攻击频率测试结果

文中也提出了防御和缓解 TCP 反射放大攻击的建议，对于被攻击的主机，自身为发起 TCP 连接，却收到响应 SYN/ACK 报文时，可以利用 RST 报文强制中断连接报文或返回 ICMP 端口不可用信息，这样的手段能够阻止部分放大器继续发送攻击报文。

本文是目前找到针对 TCP 反射放大的唯一研究，文中对于 TCP 反射放大攻击的可行性进行了较为全面的分析，结果表明利用 TCP 进行反射放大攻击确实可行，且在选取合适的放大器类型和协议条件下可以达到较好的攻击效果，与基于 UDP 的反射放大攻击相近，但是相比 UDP 反射放大攻击，可用的放大器数量明显较少。

三． 检测方法

关于 TCP 反射放大攻击的检测方法，目前没有找到相关的研究工作，由于其与 TCP SYN 洪水攻击的相似性，对 SYN 洪水攻击的检测进行了调研。

文献[2]中作者提出 AVANT-GUARD 来应对 SYN 攻击，该方法在 SDN 节点中设置 SYN 代理来防御 SYN 洪水攻击，SYN 代理负责接收 TCP 连接建立请求，代理收到 SYN 请求时会存储 SYN 请求的信息并返回 SYN/ACK 应答，但是并不分配资源来建立连接，只有在代理收到响应的 ACK 响应后，代理才会通知 SDN 控制器建立连接，从而防止 SYN 攻击占用资源。

文献[3]中作者提出使用机器学习的方法来对多种 DDoS 攻击进行检测，文中使用支持向量机进行检测，能够识别包括 TCP SYN 洪水攻击在内的多种攻击方式，SVM 接收处理后的网络流量，将流量分类为正常流量和恶意流量。

文献[4]和[5]中采用了类型的方式来防御 SYN 洪水攻击，每个 MAC 地址发送的 SYN 报文数量被记录下来，一旦数量超过一个设定的阈值，该 MAC 地址就被加入黑名单。当 SDN 控制器收到 SYN 请求报文时，控制器会返回 SYN/ACK 报文，只有收到 ACK 报文后，这个地址才被判定为合法，并进行后续的连接。

文献[6]中作者提出了 SAFETY 方法，该方法通过计算目的 IP 地址，端口号和 TCP 标志位的熵来检测 SYN 洪水攻击的方法，并设计了能够自适应网络情况的可变阈值，当计算得到的熵小于阈值时，则认为遭到了 SYN 洪水攻击。遭到攻击时，通过固定的阈值来识别攻击中的受害者和攻击者使用的端口，发现攻击端口后就封锁这个端口直到收到来自这个端口的 ACK 响应为止。

文献[7]中作者提出了使用 TCP 超时机制和 RTT 来进行检测 SYN 攻击，当收到来自一个主机的第一个 SYN 报文时，丢弃这个报文，攻击者通常不会对攻击 SYN 报文进行重传，而正常用户会重传这个被丢弃的 SYN 报文，这一步可以对攻击进行初步过滤。收到重传的 SYN 报文时，记录下重传 SYN 报文和第一次 SYN 报文之间的 RTT 时间，并返回 SYN/ACK 响应，如果能在记录的 RTT 时间内返回 ACK 响应则正常进行 TCP 连接，如果不能，则认为是 SYN 攻击，这个连接会被放弃。

文献[8]中作者分析了 SYN 攻击的各种情况并总结了各种情况下的流量特征，通过监测网络流数据比对特征来检测攻击以及攻击类型。文献[9]中作者对 CBF（Counting Bloom Filter）结构进行改进来适应 SYN 洪水攻击的检测，该方法通过维护两个 CBF 结构来记录窗口时间内网络中出现的半开 TCP 连接数量，根据阈值来判断是否遭到 SYN 攻击。

四． 总结

利用 TCP 进行反射放大攻击从理论上是可行的，且具备形成大规模 DDoS 攻击的潜力，但是也存在放大器数量较少，放大效果不强的问题。从检测角度来说，与 SYN 洪水攻击类似，利用 TCP SYN 请求发起的攻击报文简单且没有明显特征，比较难被拦截和发现，现有的研究很少，参考 SYN 洪水攻击的检测方式，攻击发生后的检测可以根据网络流特征来进行分类，实时检测常用的方式还是通过设置半开连接的阈值。个人认为，产生此类攻击的源头还是还是 IP 仿冒和分布式的僵尸网络，高效的检测僵尸网络或许比直接检测攻击

更简单和有效，同时也能够很大程度抑制除了 TCP 反射放大攻击之外的多种 DDoS 攻击方式。

五． 参考文献

[1] Marc Kührer et al. “Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks” USENIX WOOT 2014.

[2] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, “AVANT-guard: Scalable and vigilant switch flow management in software-defined networks,” in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2013, pp. 413–424.

[3] R. Kokila, S. Selvi, and K. Govindarajan, “DDoS detection and analysis in SDN-based environment using support vector machine classifier,” in Proc. 6th Int. Conf. Adv. Comput. (ICoAC), 2014, pp. 205–210.

[4] S. Fichera, L. Galluccio, S. Grancagnolo, G. Morabito, and S. Palazzo, “OPERETTA: An OpenFlow-based remedy to mitigate TCP SYNflood attacks against Web servers,” Comput. Netw., vol. 92, no. 1, pp. 89–100, 2015.

[5] R. Mohammadi, R. Javidan, and M. Conti, “SLICOTS: An SDN-based lightweight countermeasure for TCP SYN flooding attacks,” IEEE Trans. Netw. Service Manag., vol. 14, no. 2, pp. 487–497, Jun. 2017.

[6] P. Kumar, M. Tripathi, A. Nehra, M. Conti, and C. Lal, “SAFETY: Early detection and mitigation of TCP SYN flood utilizing entropy in SDN,” IEEE Trans. Netw. Service Manag., vol. 15, no. 4, pp. 1545–1559, Dec. 2018.

[7] D. Kim, P. T. Dinh, S. Noh, J. Yi, and M. Park, “An effective defense against SYN flooding attack in SDN,” in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Jeju Island, South Korea, 2019, pp. 369–371.

[8] L. Miao, W. Ding and J. Gong, "A real-time method for detecting internet-wide SYN flooding attacks," The 21st IEEE International Workshop on Local and Metropolitan Area Networks, 2015, pp. 1-6, doi: 10.1109/LANMAN.2015.7114740.

[9] Tomáš Halagan et al. “Syn Flood Attack Detection ang Type Distinguish Mechanism Based on Counting Bloom Filter”

[10] https://www.cloudflare.com/zh-cn/learning/ddos/syn-flood-ddos-attack/

[11] https://blog.radware.com/security/2019/11/threat-alert-tcp-reflection-attacks/