Chp8 协议栈安全

沙之洲 2020012408

1. 请描述IP分片污染攻击的原理与攻击者需要具备的能力

IP 分片是位于网络层的机制，为的是解决 IP 分组在不同 MTU 网络中的传输问题。

IP 分片污染攻击时，如果攻击者能够被动的观测到或者主动触发源主机和目的主机之间发生 IP 分片，那么攻击者就可以伪装成源主机，伪造出恶意的 IP 分片，注入到源主机和目的主机之间的数据流当中，进而污染原始流量，攻击目的主机。

攻击者需要具备 IP 地址伪造的能力，因为要冒充源主机发送伪造的 IP 分片。还需要具备猜测源主机分配的 IPID 和 能够对原始报文的校验和进行欺骗的能力，因为如果校验和错误，伪造 IP 分片会被目的主机丢弃，目的主机根据 IPID 重组 IP分片。

2 结合几个针对DNS域名服务实施的DDoS攻击案例分析提升DDoS攻击防御能力的可行措施

2019 年 10 月 23 日，亚马逊 DNS 受到了 DDoS 攻击，攻击者控制大量用户对以 s3.amazonaws.com 为后缀的域名进行查询，将亚马逊权威域名服务器的资源消耗殆尽，无法响应正常的查询请求。亚马逊采取 AWS Sheild 吸收了大部分攻击流量，但是也组织了一部分正常的用户访问。

对于上述案例，可以看出，对于网络恶意流量的检测和过滤是增强对 DDoS 攻击的防御能力的有效手段，但是 AWS Sheild 也会阻止正常用户的访问，这说明可以进一步加强溯源机制，如采用真实原地址技术保障每一台接入网络的计算机的真实性，从而加快DDoS 的攻击溯源，过滤恶意流量。

2013年 8 月25日，针对 .cn 域名服务器的 DDoS 攻击，是基于大量占用链路资源造成服务器拒绝服务，峰值流量达到 15Gbps ，造成 .cn 域名解析服务瘫痪数小时。

针对上述案例，可以采用分布式部署的方式，增加权威服务器的数量，提高处理能力，提高攻击者占满所有链路带宽的难度，从而增强对 DDoS 攻击的防御能力。