针对某公司渗透测试业务的渗透测试

报告

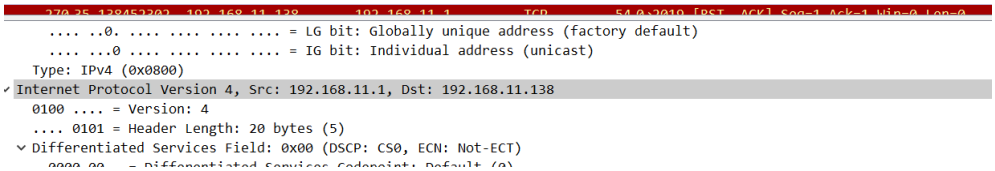
渗透时间：2019.4.01

.威胁指数：10（CVSS）

目录

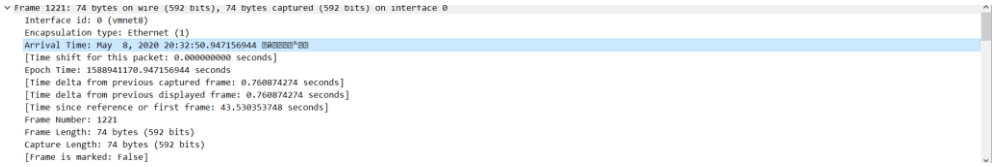
一，发现过程

经过甲方服务器运维管理人员抓取的相关数据包进行分析，分析出有重大 DDoS 洪水攻击。



经我方安全审计人员审计发现对方主机约为 1 台对甲方服务器进行大规模 DDoS 洪水攻击，并对甲方主机造成大量的网络堵塞等相关的安全问题。

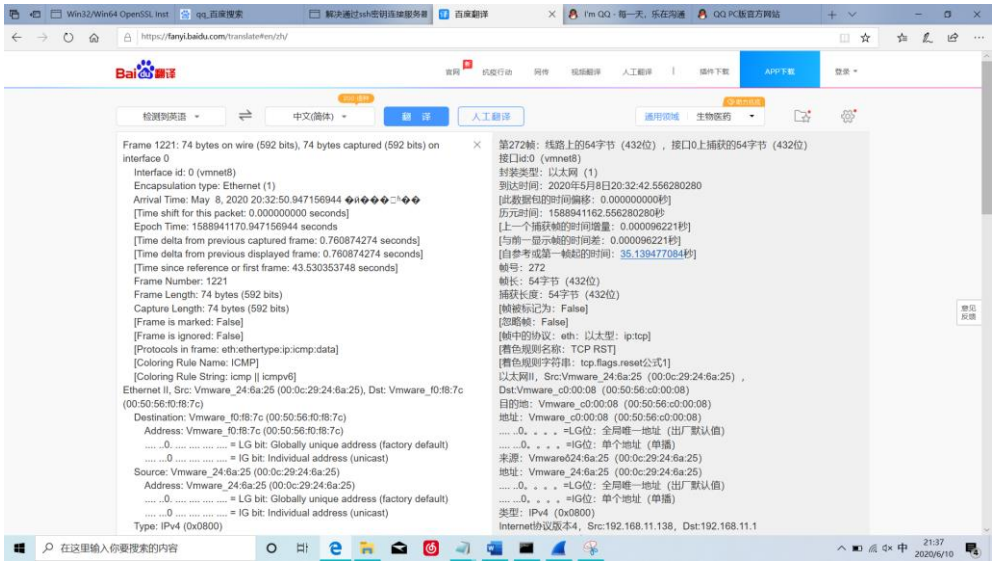
经分析可发现对方在 2020 年 5 月 8 日 20:32:42.556280280 对甲方主机发起攻击。攻击在 2020 年 5 月 8 日 20:32:42.556280280 结束攻击，并之后并无发起大 DDoS 攻击。



并之后对方主机网络开始正常访问，并可得知对方主机在 2020 年 5 月 8 日 20:32:42.556280280 时间段内还与 91.195.240.126 正常进行访问，则表明对方主机在 2020 年 5 月 8 日 20:32:42.556280280 内恢复了网络。

二，受害范围

通过我观察甲方主机是在经分析可发现对方在 2020 年 5 月 8 日 20:32:42.556280280 攻击的我们服务器，甲方服务器为 192.168.11.1 细节一点来说是线路上的 54 字节（432 位），接口 0 上捕获的 54 字节（432 位）
对方的地址就是 192.168.11.1



三，解决方法

通过我对白莲花的攻击手段我发现 甲方一定要提升公司的防火墙系统 还有该司员工的防木马技术 对于未知的东西不乱点 按时维护安全系统 该升级的时候要升级，因为黑客攻击是不可避免的 没有东西是攻不破的 重点是要时刻更新公司的安全系统 俗话说嘛：安全是唯一 安全做好了客户才放心嘛 这就是我给甲方提的建议。