

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 1

二，受害范围..... 2

三，解决方法..... 6

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。

```
270 25 129451200 192.168.11.138 192.168.11.1 TCP 54 0->2010 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ..0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
✓ Internet Protocol Version 4, Src: 192.168.11.1, Dst: 192.168.11.138
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    000 00  = Differentiated Services Codepoint: Default (0)
```

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。

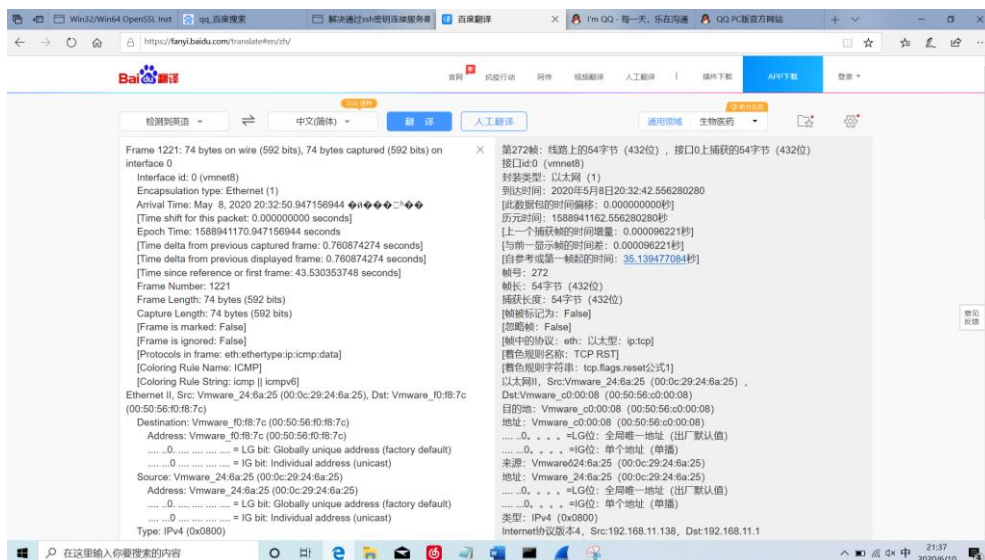
经分析可发现对方在 2020 年 5 月 8 日 20:32:42.556280280 对甲方主机发起攻击。攻击在 2020 年 5 月 8 日 20:32:42.556280280 结束攻击，并之后并无发起大 DDoS 攻击。

```
✓ Frame 1221: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
  Interface id: 0 (vmmeth)
  Encapsulation type: Ethernet (1)
  Arrival time: May 8, 2020 20:32:59.947156944 0900000000
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1588941170.947156944 seconds
  [Time delta from previous captured frame: 0.760874274 seconds]
  [Time delta from previous displayed frame: 0.760874274 seconds]
  [Time since reference or first frame: 43.538353748 seconds]
  Frame Number: 1221
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
```

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。