《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

姓名： 乔一凡 **学号：** 2015011398

作业题目：体验入侵检测

任务一 分析实验结果

使用如下命令检测 3.pcap 文件：

```
suricata -r 3.pcap -l ./
```

查看 fast.log，获取结果如下：

```
12/03/2017-01:13:59.506103  [**] [1:2019016:3] ET DOS Possible NTP DDoS
Inbound attack [**] [Classification: Attempted Denial of Service]
[Priority: 2] {UDP} 192.168.234.1:52322 -> 192.168.234.128:123
```

从上面的结果我们可以看出，suricata 识别出这可能是一次 DoS inbound 攻击，并标出时间大约在 2017 年 12 月 3 日 01:13 分左右。

通过记录，我们可以看到攻击发起者的 IP 为 192.168.234.1，使用的端口为 52322 端口。被攻击的主机 IP 地址为 192.168.234.128，被攻击端口为 123。可以看到攻击来源于局域网内部。

攻击者使用 UDP 数据包进行攻击，利用 UDP 无连接的特性，发送大量的 UDP 大包，消耗被攻击者的网络资源，实现 DoS 攻击。攻击者攻击的服务为 NTP 服务（Network Time Protocol）。该服务本身是用于同步网络中各个计算机的时间的，在这里被攻击者利用进行拒绝服务攻击。

根据网上查阅的资料，常见的 NTP 攻击是 NTP 反射放大攻击，攻击者通过伪装成被攻击者进行 NTP 查询，并通过 NTP 服务器的大量返回内容攻击被攻击者。

但是在我们这一个例子中我认为攻击方式更加简单，攻击者只是向被攻击者重复发送 NTP 数据包，达到拒绝服务攻击的效果。

任务二 分析 PCAP 包内容

使用 wireshark 进行抓包分析，对 3.pcap 进行分析。

分析结果如下：（具体见下图）

共发送了 104423 个包，其中绝大部分发送的是 NTPv2 协议的包，使用了 UDP 协议；

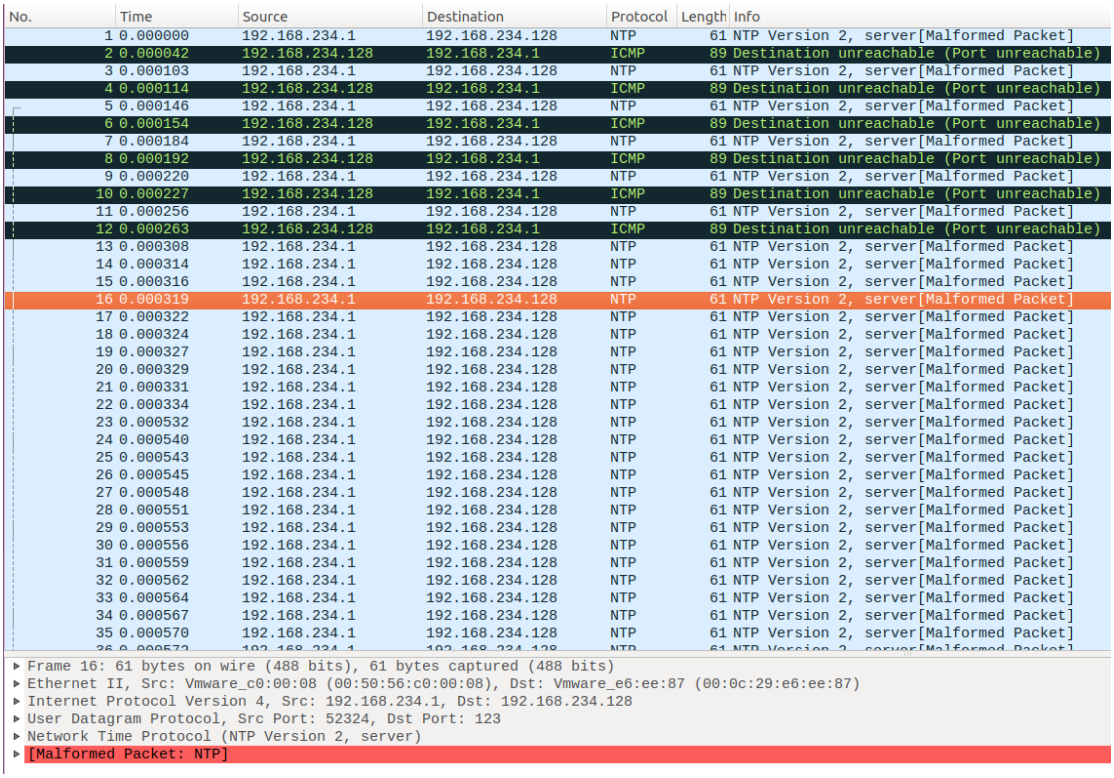
发送的源地址为 192.168.234.1，源端口主要范围为 52322~52328，目的地址为 192.168.234.128，目的端口为 123；

每个包的大小都不大，长度仅为 61，但是发送频率高，发送总量大，从而对目的地址

发起了 DoS 攻击。

查看每个包的内容，发现都是无意义的字符，具体内容为：“Today is a good day”

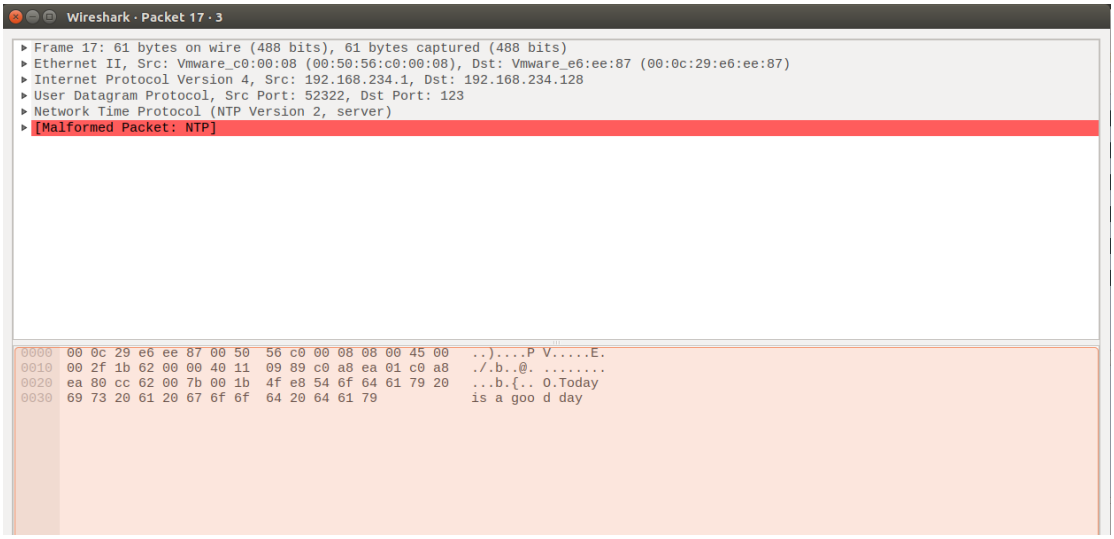
可见分析结果与 suricata 分析的完全一致。Suricata 成功地检测到了 Dos 攻击。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
2	0.000042	192.168.234.128	192.168.234.1	ICMP	89	Destination unreachable (Port unreachable)
3	0.000103	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
4	0.000114	192.168.234.128	192.168.234.1	ICMP	89	Destination unreachable (Port unreachable)
5	0.000146	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
6	0.000154	192.168.234.128	192.168.234.1	ICMP	89	Destination unreachable (Port unreachable)
7	0.000184	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
8	0.000192	192.168.234.128	192.168.234.1	ICMP	89	Destination unreachable (Port unreachable)
9	0.000220	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
10	0.000227	192.168.234.128	192.168.234.1	ICMP	89	Destination unreachable (Port unreachable)
11	0.000256	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
12	0.000263	192.168.234.128	192.168.234.1	ICMP	89	Destination unreachable (Port unreachable)
13	0.000308	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
14	0.000314	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
15	0.000316	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
16	0.000319	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
17	0.000322	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
18	0.000324	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
19	0.000327	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
20	0.000329	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
21	0.000331	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
22	0.000334	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
23	0.000532	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
24	0.000540	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
25	0.000543	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
26	0.000545	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
27	0.000548	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
28	0.000551	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
29	0.000553	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
30	0.000556	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
31	0.000559	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
32	0.000562	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
33	0.000564	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
34	0.000567	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]
35	0.000570	192.168.234.1	192.168.234.128	NTP	61	NTP Version 2, server[Malformed Packet]

```
▸ Frame 16: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
▸ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_e6:ee:87 (00:0c:29:e6:ee:87)
▸ Internet Protocol Version 4, Src: 192.168.234.1, Dst: 192.168.234.128
▸ User Datagram Protocol, Src Port: 52324, Dst Port: 123
▸ Network Time Protocol (NTP Version 2, server)
▸ [Malformed Packet: NTP]
```

包的具体内容：



Wireshark · Packet 17 · 3

```
▸ Frame 17: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
▸ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_e6:ee:87 (00:0c:29:e6:ee:87)
▸ Internet Protocol Version 4, Src: 192.168.234.1, Dst: 192.168.234.128
▸ User Datagram Protocol, Src Port: 52322, Dst Port: 123
▸ Network Time Protocol (NTP Version 2, server)
▸ [Malformed Packet: NTP]
```

```
0000  00 0c 29 e6 ee 87 00 50  56 c0 00 08 08 00 45 00   ..)....P V.....E.
0010  00 2f 1b 62 00 00 40 11  09 89 c0 a8 ea 01 c0 a8   ./.b..@. ........
0020  ea 80 cc 62 00 7b 00 1b  4f e8 54 6f 64 61 79 20   ...b.{.. O.Today
0030  69 73 20 61 20 67 6f 6f  64 20 64 61 79            is a goo d day
```