《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

姓名： 路橙 **学号：** 2015010137

作业题目：体验入侵检测

学号 2015010137 mod 3 为 2.

Part 1：分析实验结果

```
root@ubuntu:/home/suricata/Desktop/pcapfile# suricata -r 2.pcap -l ./
1/1/2018 -- 06:58:40 - <Notice> - This is Suricata version 2.0.8 RELEASE
1/1/2018 -- 06:58:40 - <Notice> - all 2 packet processing threads, 3 management threads initialized, engine started.
1/1/2018 -- 06:58:41 - <Notice> - Signal Received.  Stopping engine.
1/1/2018 -- 06:58:41 - <Notice> - Pcap-file module read 114435 packets, 7552930 bytes
root@ubuntu:/home/suricata/Desktop/pcapfile# ls
1.pcap  2.pcap  3.pcap  eve.json  fast.log  http.log  stats.log  unified2.alert.1514818707  unified2.alert.1514818720
```

```
12/03/2017-01:12:30.455015  [**] [1:0:0] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.234.1:57611 -> 192.168.234.128:69
12/03/2017-01:12:30.455355  [**] [1:0:0] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.234.1:57613 -> 192.168.234.128:69
12/03/2017-01:12:30.455407  [**] [1:0:0] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.234.1:57614 -> 192.168.234.128:69
12/03/2017-01:12:30.455443  [**] [1:0:0] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.234.1:57612 -> 192.168.234.128:69
12/03/2017-01:12:30.455488  [**] [1:0:0] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.234.1:57615 -> 192.168.234.128:69
12/03/2017-01:12:30.455568  [**] [1:0:0] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.234.1:57616 -> 192.168.234.128:69
12/03/2017-01:12:30.455570  [**] [1:0:0] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.234.1:57617 -> 192.168.234.128:69
12/03/2017-01:12:30.460858  [**] [1:0:0] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.234.1:57618 -> 192.168.234.128:69
```

DDos 攻击的端口：69（即 192.168.234.128:69）

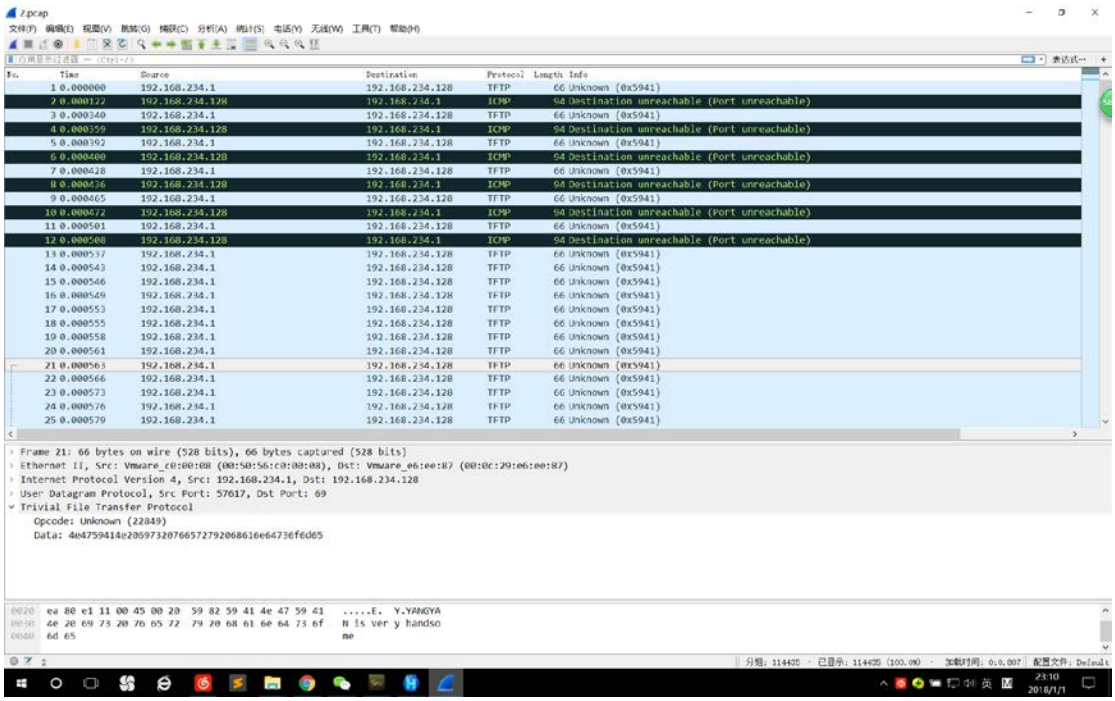
DDos 攻击的服务：SolarWinds TFTP Server Read Request（SolarWinds TFTP 服务器读取请求）

服务内容：获取通过 SolarWinds 网络工具库读取 TFTP 服务器内容的权限。

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

Part 2：分析 pcap 文件内容



源 IP： 192.168.234.128

源端口： 57611

目的 IP： 192.168.234.1

目的端口： 69

报内容： YANGYAN is ver y handsome