Session Data

Evan Misshula

emisshula@qc.cuny.edu

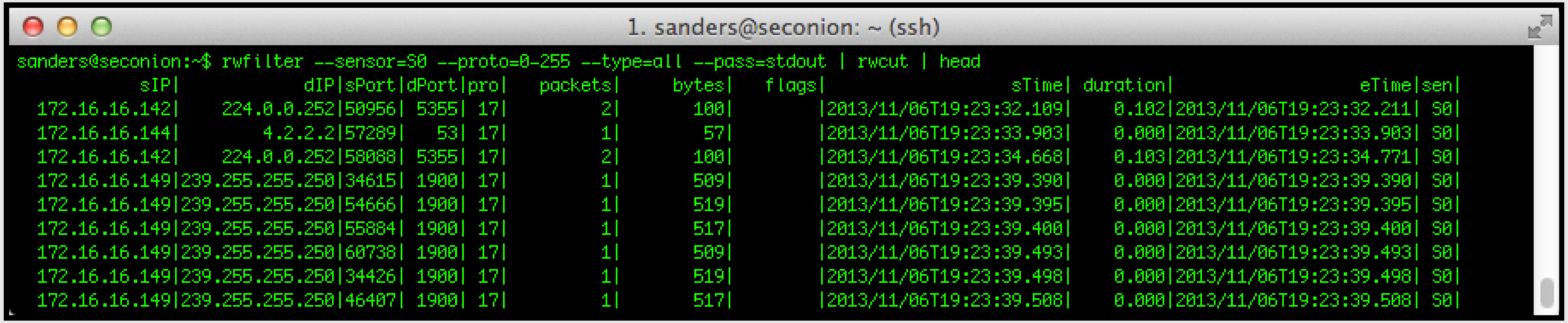
What is session data?

- Session data is the summary of the communications between two devices
- log is like the bill of a mobile phone
- Who? What? Where?

Typical report

- source ip
- destination ip
- amount of data transfered
- timestamps

Sample session data



```
sanders@seconion:~$ rwfilter --sensor=S0 --proto=0-255 --type=all --pass=stdout | rwcut | head
            sIP|            dIP|sPort|dPort|pro|   packets|     bytes|   flags|                  sTime| duration|                  eTime|sen|
  172.16.16.142|    224.0.0.252|50956| 5355| 17|         2|       100|        |2013/11/06T19:23:32.109|    0.102|2013/11/06T19:23:32.211| S0|
  172.16.16.144|        4.2.2.2|57289|   53| 17|         1|        57|        |2013/11/06T19:23:33.903|    0.000|2013/11/06T19:23:33.903| S0|
  172.16.16.142|    224.0.0.252|58088| 5355| 17|         2|       100|        |2013/11/06T19:23:34.668|    0.103|2013/11/06T19:23:34.771| S0|
  172.16.16.149|239.255.255.250|34615| 1900| 17|         1|       509|        |2013/11/06T19:23:39.390|    0.000|2013/11/06T19:23:39.390| S0|
  172.16.16.149|239.255.255.250|54666| 1900| 17|         1|       519|        |2013/11/06T19:23:39.395|    0.000|2013/11/06T19:23:39.395| S0|
  172.16.16.149|239.255.255.250|55884| 1900| 17|         1|       517|        |2013/11/06T19:23:39.400|    0.000|2013/11/06T19:23:39.400| S0|
  172.16.16.149|239.255.255.250|60738| 1900| 17|         1|       509|        |2013/11/06T19:23:39.493|    0.000|2013/11/06T19:23:39.493| S0|
  172.16.16.149|239.255.255.250|34426| 1900| 17|         1|       519|        |2013/11/06T19:23:39.498|    0.000|2013/11/06T19:23:39.498| S0|
  172.16.16.149|239.255.255.250|46407| 1900| 17|         1|       517|        |2013/11/06T19:23:39.508|    0.000|2013/11/06T19:23:39.508| S0|
```

What is industry practice?

- FPC minutes or hours
- Session months or years

Analysis Benefit

- Less cruft faster analysis
- abiltiy to zero in on what is important

Do records have a standard format?

- standard 5-tuple
  - source ip
  - destination ip
  - source port
  - destination ip
  - transport protocol

Other formats

- NetFlow v5
- NetFlow v9
- IPFIX

Termination

- Natural Timeout
- Idle Timeout
- Active Timeout

Creation

- When packet with new five tuple
  - create new record

A good exercise

- capture packet and flow
- map the packets to the flow
- flow data is a projection of packet data

Netflow

- originally a cisco spec in 1990
- provided comparison from router to other net services
- identify and summarize large amounts of traffic to simplify processes (ie ACL comparisons)

Netflow

- v5 20 fields
- v9 104 fields (supports ipV6)
- IPFIX (binary) variable length fields (supports ipV6)

Other Flow Types

- Juniper JFlow
- Citrix ApFlow
- sFlow (a sample)

Collecting Session Data

- generator
- collector

Collection can be derivative or "off the wire" Also called

- hardware
- software

Hardware

- can be done off an existing router
- can be computationally expensive
- NetFlow can be generated from any cisco router

Software

- create a daemon on the sensor to collect and forward data

Common solutions

- Fprobe (can be installed via apt-get)
- generate the flow on:
    - eth1
    - send it to 192.168.15 port 2888

```
fprobe -i eth1 192.168.1.15:2888
```

YAF (Yet another flowmeter)

- IPFIX data format
- integrates with SiLK
- IPFIX template architecture and SiLK apllication labels
- NetSA https://tools.netsa.cert.org/yaf/libyaf/yaf_silk.html

SiLK (System for Internet-Level Knowledge)

- manageable security analysis across networks
- combination of python, c and perl
- known for a good community
- packing and analysis

Packing

- ability to compress flow data into binary format

Analysis

- complex calculations and formating
  - chaining through pipes (a la regex)

Obtaining data

- generator and collector pair
- records separated by flow type
- flow types are further separated by class
  - external -> internal
  - internal -> external
  - internal -> internal
  - network architecture

Based on a configuration file

Collection process

- rwflowpack
  - parses
  - determines origin
  - stores data

rflowpack.conf

```
service rwflowpack start
```

Startup

- The startup may throw an error.
- rwflowpack checks the configuration of silk.conf and sensor.conf
  - it also won't start if not all sensors are available
- flowcap can be used if data needs to be stored and fowarded
  - preprocessor
    - other tools include
      1. rwflowappend
      2. rwpackchecker
      3. rwpollexec

SiLK flow types

- SiLK data can be organized
  - In: inbound
  - Out: outbound
  - Int2int: internal
  - Ext2ext: external
  - Inweb: inbound on port 80, 443, 8080
  - OutWeb: outbound on port 80, 443, 8080
  - Inicmp: inbound icmp
  - Outicmp: outbound icmp
  - Other:

SiLK Analysis Toolset

- 55 seperate tools
- rwfilter most common
  - select statement
  - compound statements applied through pipes

Filtering flow data with rwfilter

- selecting session data
- important for narrowing network forensics
  - find the offending source ip
    - rwfilter –anyaddress –start-date –end-date –type –pass=stdout
    - pass this to rwcut
    - a sample statement follows

```
rwfilter --anyaddress=1.2.3.4 --start-date=2013/06/22:11 --end-date=2013/06/22:11 --type=a
```

This captures from 11am to 1pm

Another scenario

- Suspicious ip 6.6.6.6 is receiving data after midnight
- Get the size of the data

```
rwfilter --anyaddress=6.6.6.6 --start-date=2013/06/22:00  --type=all --pass=stdout | rwcut
```

Restricted to a port

or we can restrict it to the https port:

```
rwfilter --anyaddress=6.6.6.6 --start-date=2013/06/22:00  --aport=443 --type=all --pass=st
```

Restricted to a single conversation

or to restrict it to one conversation

```
rwfilter --anyaddress=6.6.6.6 --start-date=2013/06/22:00  --saddress=192.168.1.100 --daddr
```

Piping

- The pipe to rwcut changes binary to human readable
- Rwcount returns counts
  - How many users?
  - When is traffic busiest

Records over time

```
rwfilter  --start-date=2013/06/22 --proto=0-255 --type=all --pass=stdout | rwcount  --bin-
```

Created by Evan Misshula.