Cyber Sandwich

Generating Custom CSV Reports With Tshark

November 16, 2016
Networking
networkingreportingtsharkwireshark

Tshark is a network protocol analyzer. Tshark is the command line version of the popular networking tool Wireshark. I will be going over some useful commands to filter pcap files and generate custom CSV reports with any fields of the packet data.

Useful filtering options

-r <infile> read data from input file

-Y <display filter> Filter display packets. This uses the same syntax as the Wireshark GUI filter

-G [<report type>] List glossary

-o <preference>:<value> set a preference value

-T fields|pdml|ps|psml|text

-e <field> add a field to display. This is required when -T fields is used. In order to display columns from Wireshark you must prefix the column with _ws.col.*

-E <field print option> format how fields are printed.

Examples

Use the -G column-formats to list all possible display columns. This allows you to name fields to display in your report using the -o option to overwrite the default value

```
# tshark -G column-formats
...
%p Protocol
%Rt Relative time
%rct Relative time (conversation)
%s Source address
%S Source port
...
```

Use the -o option to customize the columns that are displayed by tshark and assign names to the columns for the custom report. The following command reports the source and destination IP address, destination port, and protocol used.

```
# tshark -r sample.pcap -o'column.format:"Dport","%D","Protocol","%p"' -T fields -E separator=, -E
header=y -e eth.src -e ip.dst -e _ws.col.Dport -e _ws.col.Protocol > output.csv
#more output.csv
ip.src,ip.dst,_ws.col.Dport,_ws.col.Protocol
172.16.100.150,75.75.75.75,53,DNS
172.16.100.150,172.16.100.100,80,TCP
172.16.100.100,172.16.100.150,53539,TCP
172.16.100.150,172.16.100.100,80,TCP
172.16.100.150,172.16.100.100,80,HTTP
```

For example the following command displays the source IP, destination IP, and the Info fields of packets using the HTTP protocol and writes the file to a csv.

```
# tshark -r sample.pcap -Y "http" -o'column.format:"Info","%i"'-T fields -E separator=, -E header=y -
e ip.src -e ip.dst -e _ws.col.Info > output.csv
# more output.csv
ip.src,ip.dst,_ws.col.Info
172.16.100.150,172.16.100.100,GET / HTTP/1.1
172.16.100.100,172.16.100.150,HTTP/1.1 304 Not Modified
172.16.100.150,172.16.100.100,GET /styles.css HTTP/1.1
172.16.100.100,172.16.100.150,HTTP/1.1 304 Not Modified
```

Next Post
Previous Post

- Programming
- Reverse Engineering

- **Friends**

  - Zeall
  - Lucas
  - Travis

- Home
- About Me