
ATTACK
DEFENSE
by PentesterAcademy

Name	Read Filters and HTML Export
URL	https://www.attackdefense.com/challengedetails?cid=49
Type	Traffic Analysis: Tshark Fu

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. Copy the first 10 HTTP packets from HTTP_traffic.pcap to a new file First10.pcap

This requires the use of read filters in tshark. The following command ensures only HTTP packets are read from the file.

Command: tshark -r HTTP_traffic.pcap -2 -R http -c 10

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -2 -R http -c 10
    1   4.166998 192.168.252.128 ? 54.239.32.8  HTTP 904 GET / HTTP/1.1
    2   4.168852 192.168.252.128 ? 54.239.39.114 HTTP 1150 POST /1/batch/1/OE/ HTTP/1.1  (text/plain)
    3   4.472330 54.239.39.114 ? 192.168.252.128 HTTP 431 HTTP/1.1 204 No Content
    4   5.060440 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/412maSA0fuL._AC_SY200_.jpg HTTP/1.1
    5   5.062201 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41wuVnAeedL._AC_SY200_.jpg HTTP/1.1
    6   5.068393 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/412OwlOMxPL._AC_SY200_.jpg HTTP/1.1
    7   5.068453 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/316zh6kkqML._AC_SY200_.jpg HTTP/1.1
    8   5.068562 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41O1oRMP6pL._AC_SY200_.jpg HTTP/1.1
    9   5.069236 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41w3V6ilQPL._AC_SY200_.jpg HTTP/1.1
   10   5.244323 52.84.108.225 ? 192.168.252.128 HTTP 6840 HTTP/1.1 200 OK  (JPEG JFIF image)
student@attackdefense:~$
```

Save these packets into a new file First10.pcap

Command: tshark -r HTTP_traffic.pcap -Y http -c 189 -w First10.pcap

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y http -c 189 -w First10.pcap
student@attackdefense:~$
```

Q2. Print full details (all fields should be printed) of all 10 packets in First10.pcap

Command: tshark -r First10.pcap -V

```
student@attackdefense:~$ tshark -r First10.pcap -V
Frame 1: 904 bytes on wire (7232 bits), 904 bytes captured (7232 bits) on interface 0
    Interface id: 0 (unknown)
        Interface name: unknown
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 20, 2016 07:38:28.678418000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1466408308.678418000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 904 bytes (7232 bits)
    Capture Length: 904 bytes (7232 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
Ethernet II, Src: Vmware_07:40:41 (00:0c:29:07:40:41), Dst: Vmware_e5:4d:16 (00:50:56:e5:4d:16)
    Destination: Vmware_e5:4d:16 (00:50:56:e5:4d:16)
        Address: Vmware_e5:4d:16 (00:50:56:e5:4d:16)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Vmware_07:40:41 (00:0c:29:07:40:41)
        Address: Vmware_07:40:41 (00:0c:29:07:40:41)
```

Q3. Export all 10 packets in First10.pcap into PDML format

Command: tshark -r First10.pcap -T pdml > http.xml

```
student@attackdefense:~$ tshark -r First10.pcap -T pdml > http.xml
student@attackdefense:~$
student@attackdefense:~$ head -20 http.xml
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xsl" href="pdml2html.xsl"?>
<!-- You can find pdml2html.xsl in /usr/share/wireshark or at https://code.wireshark.org/review/gitweb?p=wireshark.git;a=blob_plain;f=pdml2html
.xsl. -->
<pdml version="0" creator="wireshark/2.6.1" time="Wed Nov  7 20:13:19 2018" capture_file="First10.pcap">
<packet>
  <proto name="geninfo" pos="0" showname="General information" size="904">
    <field name="num" pos="0" show="1" showname="Number" value="1" size="904"/>
    <field name="len" pos="0" show="904" showname="Frame Length" value="388" size="904"/>
    <field name="caplen" pos="0" show="904" showname="Captured Length" value="388" size="904"/>
    <field name="timestamp" pos="0" show="Jun 20, 2016 07:38:28.678418000 UTC" showname="Captured Time" value="1466408308.678418000" size="904"
/>
  </proto>
  <proto name="frame" showname="Frame 1: 904 bytes on wire (7232 bits), 904 bytes captured (7232 bits) on interface 0" size="904" pos="0">
    <field name="frame.interface_id" showname="Interface id: 0 (unknown)" size="0" pos="0" show="0">
      <field name="frame.interface_name" showname="Interface name: unknown" size="0" pos="0" show="unknown"/>
    </field>
    <field name="frame.encap_type" showname="Encapsulation type: Ethernet (1)" size="0" pos="0" show="1"/>
    <field name="frame.time" showname="Arrival Time: Jun 20, 2016 07:38:28.678418000 UTC" size="0" pos="0" show="Jun 20, 2016 07:38:28.67841800
0 UTC"/>
    <field name="frame.offset_shift" showname="Time shift for this packet: 0.000000000 seconds" size="0" pos="0" show="0.000000000"/>
    <field name="frame.time_epoch" showname="Epoch Time: 1466408308.678418000 seconds" size="0" pos="0" show="1466408308.678418000"/>
    <field name="frame.time_delta" showname="Time delta from previous captured frame: 0.000000000 seconds" size="0" pos="0" show="0.000000000"/
>
student@attackdefense:~$
```

Q4. Convert the PDML export into a HTML file. Use lynx or browsh to view them.

Command: xsltproc /usr/share/wireshark/pdml2html.xsl http.xml > http.html

```
student@attackdefense:~$ xsltproc /usr/share/wireshark/pdml2html.xsl http.xml > http.html
student@attackdefense:~$
student@attackdefense:~$ head -20 http.html
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>poor man's Wireshark</title>
<script src="http://ajax.googleapis.com/ajax/libs/dojo/1.4/dojo/dojo.xd.js" type="text/javascript"></script><script type="text/javascript">
function set_node(node, str)
{
  if(dojo.isString(node))
    node = dojo.byId(node);
  if(!node) return;
  node.style.display = str;
}
function toggle_node(node)
{
  if(dojo.isString(node))
    node = dojo.byId(node);
  if(!node) return;
  set_node(node, (node.style.display != 'none') ? 'none' : 'block');
}
function hide_node(node)
student@attackdefense:~$
```

Q5. How many HTTP GET request packets are present in HTTP_traffic.pcap?

Command: tshark -r HTTP_traffic.pcap -Y "http.request.method==GET" | wc

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y "http.request.method==GET" | wc
    679    6111  136249
student@attackdefense:~$
```

References:

1. Tshark (https://www.wireshark.org/docs/man-pages/tshark.html)
2. Wireshark (https://www.wireshark.org/)