TryHackMe: TShark Challenge II: Directory

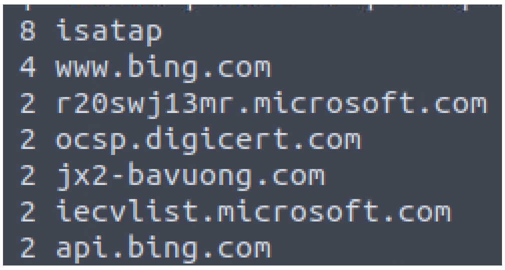
The following is a writeup for the TShark Challenge II: Directory room. This challenge involved using TShark to investigate a pcap. It was another simple challenge that is very handy when first learning how to use the tool.

Scenario: An alert has been triggered: “A user came across a poor file index, and their curiosity led to problems”. The case was assigned to you. Inspect the provided directory-curiosity.pcap and retrieve the artifacts to confirm that this alert is a true positive. Your tools: TShark, VirusTotal.

What is the name of the malicious/suspicious domain?

To find name lof the malicious/suspicious domain address, we can extract the dns.query.name field like as follows:

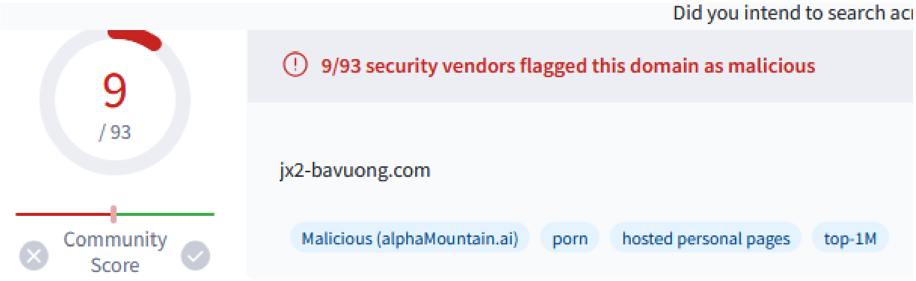
- tshark -r directory-curiosity.pcap -T fields -e dns.qry.name | awk NF | sort -r | uniq -c | sort -r



```
8 isatap
4 www.bing.com
2 r20swj13mr.microsoft.com
2 ocsp.digicert.com
2 jx2-bavuong.com
2 iecvlist.microsoft.com
2 api.bing.com
```

- awk NF removes the empty lines
- sort -r recursively sorts before handling the values
- uniq -c shows unique values and calculates the number of occurrences for each value, and
- sort -r shows the output from high occurrence to low occurrences.

Let’s investigate some of these domains by using VirusTotal:

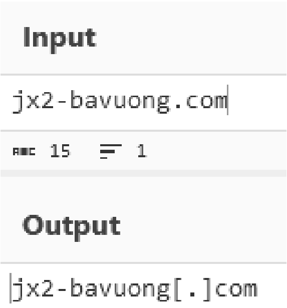


Did you intend to search ac

9/93 security vendors flagged this domain as malicious

jx2-bavuong.com

As you can see, the domain in the above image was flagged as malicious by 9 security vendors, let’s now use cyberchef to defang the URL:



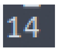
```
jx2-bavuong.com
```

```
jx2-bavuong[.]com
```

What is the total number of HTTP requests sent to the malicious domain?

As explained in the hint, we can use the http.request.full_uri field to answer this question. All we need to do is use a display filter like as follows:

- tshark -r directory-curiosity.pcap -Y 'http.request.full_uri contains "jx2-bavuong.com"' -T fields -e http.request.full_uri | wc -l



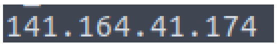
```
14
```

This outputs 14, which means 14 HTTP requests were sent to the malicious domain.

What is the IP address associated with the malicious domain? Enter your answer in a defanged format.

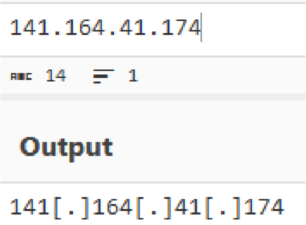
All we need to do is slightly modify the previous command to find the IP address associated with the malicious domain. We can do this by entering:

- tshark -r directory-curiosity.pcap -Y 'http.request.full_uri contains "jx2-bavuong.com"' -T fields -e ip.dst | sort | uniq



```
141.164.41.174
```

You then need to defang the IP address, you can do this manually or use Cyberchef:



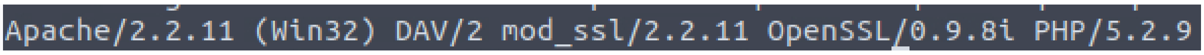
```
141.164.41.174
```

```
141[.]164[.]41[.]174
```

What is the server info of the suspicious domain?

The server info can be found in the http.server field, so all we need to do is extract this field if it relates to the malicious domain we identified earlier on. This can be done by entering:

- tshark -r directory-curiosity.pcap -Y 'http contains "jx2-bavuong.com"' -T fields -e http.server | awk NF | sort | uniq



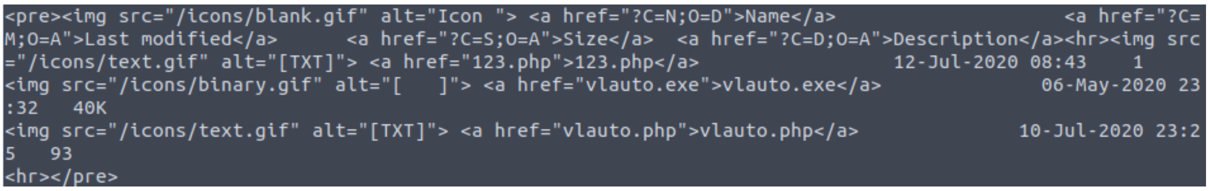
```
Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
```

Follow the “first TCP stream” in “ASCII”. Investigate the output carefully. What is the number of listed files.

To follow the first TCP stream, we can enter:

- tshark -r directory-curiosity.pcap -z follow,tcp,ascii,0 -q

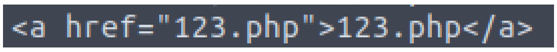
If you inspect the output carefully, you can find the number of listed files in the following screenshot:



```
<pre><img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name</a>                    <a href="?C=
M;O=A">Last modified</a>      <a href="?C=S;O=A">Size</a>  <a href="?C=D;O=A">Description</a><hr><img src
="/icons/text.gif" alt="[TXT]"> <a href="123.php">123.php</a>                    12-Jul-2020 08:43    1
<img src="/icons/binary.gif" alt="[   ]"> <a href="vlauto.exe">vlauto.exe</a>                06-May-2020 23
:32   40K
<img src="/icons/text.gif" alt="[TXT]"> <a href="vlauto.php">vlauto.php</a>                10-Jul-2020 23:2
5   93
<hr></pre>
```

What is the filename of the first file? Enter your answer in a defanged format.

The filename of the first file defanged is 123[.]php:

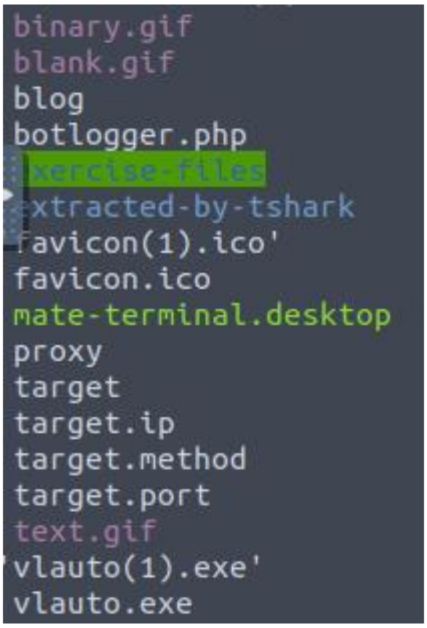


```
<a href="123.php">123.php</a>
```

Export all HTTP traffic objects. What is the name of the downloaded executable file? Enter your answer in a defanged format.

To extract all the HTTP objects and save it to “extracted-by-tshark” in my case, enter the following command:

- tshark -r directory-curiosity.pcap --export-objects http,/home/ubuntu/Desktop -q

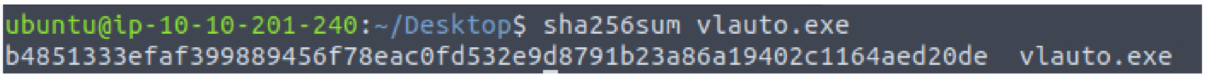


```
binary.gif
blank.gif
blog
botlogger.php
xercise-files
xtracted-by-tshark
favicon(1).ico'
favicon.ico
mate-terminal.desktop
proxy
target
target.ip
target.method
target.port
text.gif
'vlauto(1).exe'
vlauto.exe
```

The name of the downloaded executable in defanged format is vlauto[.]exe.

What is the SHA256 value of the malicious file

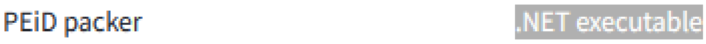
We can use the sha256sum command in the terminal to hash the file:



```
ubuntu@ip-10-10-201-240:~/Desktop$ sha256sum vlauto.exe
b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aed20de  vlauto.exe
```

Search the SHA256 value of the file on VirusTotal. What is the PEiD packer value?

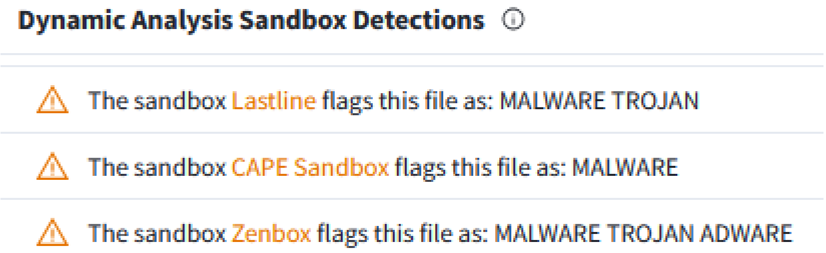
After entering the hash into VirusTotal, navigate to the details tab and look at the last field under the Basic properties heading:



PEiD packer .NET executable

What does the LastLine Sandbox flag this as?

Navigate to the behaviour tab in VirusTotal, if you look under the Dynamic Analysis Sandbox Detections heading, we can find the answer:



Dynamic Analysis Sandbox Detections

⚠ The sandbox Lastline flags this file as: MALWARE TROJAN

⚠ The sandbox CAPE Sandbox flags this file as: MALWARE

⚠ The sandbox Zenbox flags this file as: MALWARE TROJAN ADWARE

MALWARE TROJAN is the answer.

The TShark Challenge II: Directory room provides a comprehensive exercise in using TShark to analyse network traffic and identify malicious activity. By methodically examining the pcap file, I was able to identify the suspicious domain and executable downloaded from said domain. I hope this writeup can be of use for someone else doing the SOC Analyst 1 path on TryHackMe.