TryHackMe: TShark Challenge 1: Teamwork

The following writeup covers the TShark Challenge 1 room which is part of the SOC analyst 1 path. This room involved using TShark to investigate a pcap. It was a really simply yet fun way to practice with TShark, and it should only take around 10-20 minutes even for a complete beginner.

Scenario: An alert has been triggered: "The threat research team discovered a suspicious domain that could be a potential threat to the organisation". The case was assigned to you. Inspect the provided teamwork.pcap and create artefacts for detection tooling. Your tools: TShark, VirusTotal.

What is the full URL of the malicious/suspicious domain address. Enter your answer in defanged format.

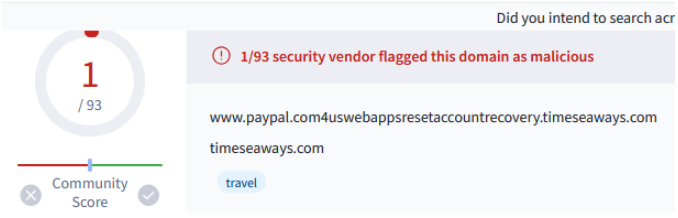
To find the full URL of the malicious/suspicious domain address, we can extract the http.host field like as follows:

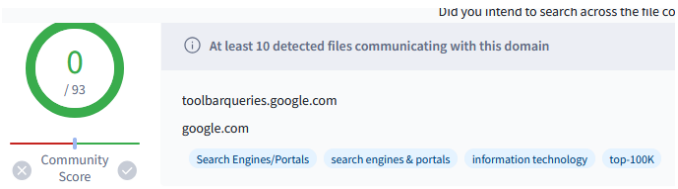
- tshark -r teamwork.pcap -T fields -e http.host -e ip.dst | awk NF | sort -r | uniq -c | sort -r

```
ubuntu@ip-10-10-71-66:~/Desktop/exercise-files$ tshark -r teamwork.pcap -T fields -e http.host | awk NF | sort -r | uniq -c | sort -r
     21 www.paypal.com4uswebappsresetaccountrecovery.timeseaways.com
      1 toolbarqueries.google.com
```

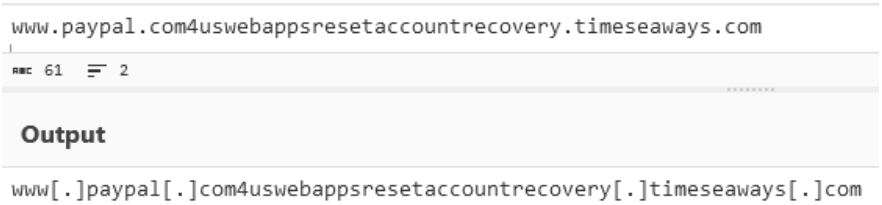
- awk NF removes the empty lines
- sort -r recursively sorts before handling the values
- uniq -c shows unique values and calculates the number of occurrences for each value, and
- sort -r shows the output from high occurrence to low occurrences.

Even though the answer is obvious, let's check the domains by using VirusTotal:





Based off of this, we can assume that the paypal link is malicious, let's now defang it using Cyberchef and the defang URL recipe:



Note, you could also find the answer by extracting the dns.qry.name field to see domain names that have been resolved.

When was the URL of the malicious/suspicious domain address first submitted to VirusTotal?

Which known service was the domain trying to impersonate?

The domain is trying to impersonate PayPal.

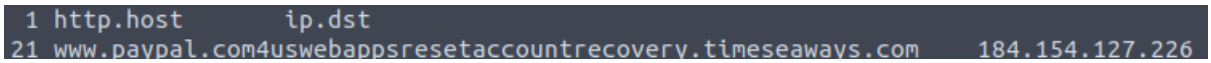
What is the IP address of the malicious domain?

To find the associated IP address, we can use a display filter to only output http traffic related to the malicious domain and extract only the http.host and ip.dst fields like as follows:

- tshark -r teamwork.pcap -Y 'http.host == "www.paypal.com4uswebappsresetaccountrecovery.timeseaways.com"' -T fields -e http.host -e ip.dst | awk NF | sort -r | uniq -c | sort -r

If you want the output to be more readable, you can enter the following:

- tshark -r teamwork.pcap -Y 'http.host == "www.paypal.com4uswebappsresetaccountrecovery.timeseaways.com"' -T fields -e http.host -e ip.dst -E header=y | awk NF | uniq -c



This let's you see the heading for the fields.

What is the email address that was used?

To identify the email address used, we can search for HTTP post requests that would indicate show us what the victim posted to the malicious domain. We can do this by using the following:

- tshark -r teamwork.pcap -Y "http.request.method == POST" -T fields -e http.host -e http.request.uri -e urlencoded-form.key -e urlencoded-form.value

You can see the email in the second POST request:

```
johnny5alive@gmail.com
```

Make sure to defang it like as follows: johnny5alive[at]gmail[.]com

The TShark Challenge 1, part of the SOC analyst 1 path on TryHackMe, provided a practical and engaging experience in using TShark to analyse pcap files. The challenge scenario involved investigating a suspicious domain to determine its threat level and gather necessary artefacts for detection tooling. Throughout this challenge, we utilised TShark to extract and analyse various fields within the pcap file. By identifying the http.host and ip.dst fields, we pinpointed the suspicious domain which was masquerading as PayPal. The investigation further revealed the domain's first submission to VirusTotal and its associated IP address. Additionally, we identified an email address used in a POST request, defanged using CyberChef to maintain safe handling of the data.