PROJECT 1

DESCRIPTION

Run Traffic Analysis attacks against https traffic.

INPUT

The Packet Trace files for the given URLs will be given.

INTENTION

1. To match the packet trace files given with the given URLs.

2. packet_dump file - raw data of captured packets.

3. packet_trace file - time from the beginning of the packet exchange, length of the packet, direction of the packet (in/out).
The packet_trace file will look like:

```
00:00:00.000000 0 in
00:00:00.000056 0 out
00:00:00.000897 201 out
00:00:00.134478 0 in
00:00:00.134523 0 out
00:00:00.135007 201 out
00:00:00.243595 0 in
00:00:00.262097 1448 in
00:00:00.262118 0 out
```

MEASUREMENTS

1. Clear the cache of browser (say, firefox).
2. Connect to URL using firefox browser using 'firefox –url sample.com'.
3. Use tcpdump to get packet dump.
4. Limit the tcpdump to listen for 10 seconds and the domain in the URL.
5. Use timeout to listen for 10 seconds to the packets.
6. Use tcpdump filter 'port https' to listen to https.

7. Use tcpdump filter 'src or dst <domain_name>' to listen to the particular domain name and get dump of packets having source or destination of that domain.

```
   '`sudo timeout --kill-after 10 10 tcpdump -G 5 -W 1 -w filename.pcap port https and src or dst sample.com'
```

8. Store the packet dump into a file using tcpdump option '-w filename.pcap'
9. Read from the .pcap file using 'sudo tcpdump -r filename.pcap'
10. Close the browser before getting packet dump for the next URL.

INSTRUCTIONS

1. Record the packet dump.
2. Get the packet trace from the packet dump, extracting the time (HH:MM:SS.000000), length of packet (bytes), direction (in/out). For example, if the packet is from your machine to https, the direction will be out, and vice verca.
3. Match given packet traces with the packet traces of URLs using any suitable method.
4. Store the index of matched packet trace file in the output file against URL index.

OUTPUT

The expected output should be a file (say, matched_traces.txt), containing the index of URL. The line index of the output file will be the packet_trace file index, and the number in each line will be the index of the matched URL.

For example, the first line of the output file will give the URL index that matched the packet_trace_0.txt, the second line in the output file will correspond to the URL index that matched the packet_trace_1.txt, and so on.

Sample Output file -

```
   3
   11
   9
   5
   33
   0
```