TLS/SSL Analysis

SUBTASK-1

Create a python program to obtain a collection of TLS certificates. You dont need to save every field of the certificate , but you should consider which fields might be useful for forensics/analytics later on. There is no required number of certificates, but you will need a large collection for the higher level machine learning tasks. Submit a document containing the following.

1. Your code and a screenshot of it running.
2. A description of what part of the certificates you have saved.
3. A print out of all the certs you have collected.

You may find the following code helpful in getting started.

Listing 1: Code Skeleton

```
1
2  import ssl
3  hostname='www.google.com'
4  port=443
5
6  f = open('cert.der','wb')
7  cert = ssl.get_server_certificate((hostname, port))
8  f.write(ssl.PEM_cert_to_DER_cert(cert))
9  f.close()
10
11
12 or alternatively
13
14 # Import modules
15 import socket
16 import pyshark
17 # Docs: https://github.com/KimiNewt/pyshark/
18 from pprint import pprint
19
20
21 data = pyshark.FileCapture(unipcap.pcap)
22
23 # Loop through each item (packet)
24 for pkt in data:
25     if TLS in pkt:
```

```
26          # Look for attribute of x509
27          if hasattr(pkt['TLS'], 'x509sat_utf8string'):
28               print(pkt[TLS])
29               pprint(dir(pkt['TLS']))
30               print(pkt['TLS'].x509sat_utf8string)
31               print(NEW CERT)
```

SUBTASK 2

Collect malware certificates for later use. In the above task you have collected a training set of valid certificates. Now we need a collection of malicious certificates to compare with. There are different ways you could build this collection. One way would be to visit https://sslbl.abuse.ch/(you may find it helpful to sort by number of times detected), and then use https://crt.sh/ to obtain the certificates. You could do this by hand, or build a script to do it. There are also collection of certificates online, such as (https://github.com/lhaagsma/sslblacklist). Collect at least 100 malicious certificates. Once you have a collection of the certs you will need to write a python script that can parse them and obtain the fields of interest.

Submit a report containing

1. Where you collected the certificates from.
2. What your method of collecting them was.
3. Your code parsing the certs.