Computer Networking – Bonus assignment

Submission requirements

1. **HW2 is to be performed in the same groups of <u>two</u> and submitted until 18/05/2021, 23:55.**
2. **The link to Drive must be submitted to Moodle and must include:**
    a. **The .txt file including all the team members' full names and IDs.**
    b. **The assignment simulation and its description including the structure of the lab.**
    c. **The detailed ReadMe file describing the process and the content of each file (for examples, what each pcap file contains, what actions were performed to generate the traffic (Web browsing, file transfer using DNS tunnel, etc.)**
3. **As it is a bonus, no late submissions are possible and no requests of adding team numbers will be allowed.**
4. **The bonus is up to 15 points to the final grade in the Computer Networking Course Spring-2021.**
5. **The project deals with creating DNS tunnels inside DoH connections.**
6. **Questions can be asked (as usual) by emailing me: alonhkoz@ac.sce.ac.il**

Goal

The goal of the assignment is to detect (classify) DNS tunnels inside DoH connections with mixed traffic (benign DoH and DNS tunnels over DoH).

a. DNS Tunnel = encapsulating TCP connection into DNS queries (requests and responses)
b. Malicious traffic = a DNS tunnel, e.g., covert tunnel
c. DoH proxy, which translates classical unencrypted DNS traffic into encrypted DoH

Task

Install DNS tunneks to generate traffic. For example, DNScat, iodine for data exfiltration (and data exfiltration tools in Canadian dataset) (see below).

a. **The following are the programs used in the DoHBrw dataset from CIC (Canadian dataset can be found at https://www.unb.ca/cic/datasets/dohbrw-2020.html):**
   - Dns2tcp (https://github.com/alex-sector/dns2tcp)
   - DNScat2 (https://github.com/iagox86/dnscat2)
   - Iodine (https://github.com/yarrick/iodine)

The list of encrypted DNS proxies can be found here:
https://dnscrypt.info/implementations

The situation we try to simulate:

There is one proxy in LAN, which is used by multiple users. One of the users is using DNS tunneling tools for malicious purposes.

Generating Data - Frequency:

a. One hour a day to be repeated some other day but at a different time, different times a day, and different days in a week (especially weekends are highly encouraged!).
b. Check the delays during different times of the day.
c. Divide between the team partners what network you use for generating the data – Wi-Fi or Ethernet. Important: the workshare and workload must be equal for both types of network!

Generating Data – simulation process:

a. Running DoH/DNS proxies, capturing with Wireshark or TCPDump
b. Capturing the traffic before the proxy and behind the proxy, before the encryption (DNS) and after the encryption (DoH).
c. Annotate the traffic with time stamps. E.g., Provide a list of labels, like “DNS tunneling started at X time”
d. Split DoH connection into time slots and for each of them to assign the class: "benign" / "tunnel" / "none" (when there is no DoH activity)
e. Export TLS keys if possible and export the keys in a separate file. Hint: check the environment variable SSLKEYLOGFILE. It works on major OSs.

Generating Data – Volume:

f. Flow generation - 100000 flows of traffic for classifying the DNS tunnel, i.e., you must have many flows (e.g. at least 3000) for each kind of tunnel.
g. You also have to generate the similar number of benign flows. These flows do not contain any tunneling traffic.
h. One group have to use a different DNS tunneling tool and a different proxy and different networks (Ethernet and Wi-Fi).

Simulation scenarios required:

Tool	**Proxy**	**Link type**	**Resolver**
Dns2tcp	DNSCrypt-Proxy	Ethernet	Google
Iodine	DNSCrypt-Proxy	Ethernet	Google
DNScat2	DNSCrypt-Proxy	Ethernet	Google
DNS2tcp	DNSCrypt-Proxy	Ethernet	Cloudflare
Dns2tcp	DoH Proxy	Ethernet	Cloudflare
Iodine	DoH Proxy	Ethernet	Cloudflare
DNScat2	DoH Proxy	Ethernet	Cloudflare
Dns2tcp	DoH Proxy	Wifi	Google

Iodine	DoH Proxy	Wifi	Google
DNScat2	DoH Proxy	Wifi	Google
Dns2tcp	DNSCrypt-Proxy	Wifi	Cloudflare
DNS2tcp	DoH Proxy	Wifi	Cloudflare
Iodine	DNSCrypt-Proxy	Wifi	Cloudflare
DNScat2	DNSCrypt-Proxy	Wifi	Cloudflare

1. **Each group should send me email and I will choose 2 lines from the table to work on.**
2. **The sooner you send the email, the sooner you can start working on the bonus assignment.**