בס"ד

Lab #5: DNS Cache Poisoning

Setup:

- Create an additional machine using the `clone` option of VBox
  - If you already have one from previous lab… use it
- Install a DNS server and supporting libraries:
  - `sudo apt-get install bind9 dnsutils bind9-doc`
- Make sure the server is running:
  - `service bind9 status|start|restart`
  - Test your server to see that it is configured correctly

Tasks:

- Compare MiTM attack with and without DNSSEC working
  - You need to turn DNSSEC OFF
    - edit `/etc/bind/named.conf.options`
  - Position your attacker between the DNS and its outgoing queries
    - Capture or sniff the query and return a legal, yet spoofed response (a response that WILL be accepted as legitimate by the DNS server).
  - Do the same with DNSSEC turned ON

Pointers:

- Think how and where you plan to position your MiTM
  - You need to create a configuration such that you are placed in the middle.
    - **Notice:** This isn't the classical DNS cache poisoning attack described during the lectures. You ARE allowed to **manually** place your attacker IN THE MIDDLE.

Additional challenge (bonus 20%):

- Carryout an additional preliminary attack to place yourself in the middle **automatically**.

Deliverables:

- A zipped file containing:
  - Your code (.py)
  - A Document explaining
    - The main parts of your code

- The cache file from your server machine showing that the address for `www.jct.ac.il` has been spoofed.
  - **You may not edit the file manually**
- On which message does your spoofing not work when DNSSEC is turned on **(for a DNSSEC enabled site)**

Note:

- You may NOT download or copy code from internet !!
- Searching the internet with specific programming question IS allowed.