netsec-dns-lab

To **start the lab**:

1. go into the laboratory directory:

- `cd ./lab`

2. start the lab

- `kathara lstart`

To **connect to a device** you can just type `kathara connect {DEVICE_NAME}`. The available devices are:

- `attacker`: where you have all the tools to perform the attack;
- `victim`: the victim of the attack. Here you will be able to check if the attack was successful;
- `rec_dns`: the recursive DNS the victim will query;
- `authoritative_dns`: the real authoritative DNS for *example.com*;
- `malicious_dns`: the attacker's DNS, set up to be authoritative for *example.com*;
- `root_dns`: the root DNS of this network topology.
- others, that shouldn't be useful for the purpose of this lab.

Example: `kathara connect attacker`.

To perform the **cache poisoning attack**:

1. On the authoritative DNS device, set delay with: `tc qdisc add dev eth0 root netem delay 1500ms`
2. Edit `./shared/cache-poisoning.cpp` with `vscode`: `code ./shared`
3. On the attacker's device, compile your code: `g++ -o cache-poisoning /shared/cache-poisoning.cpp -ltins`
4. On the attacker's device run the script: `./cache-poisoning`
5. On the victim's device, verify that foo.example.com resolves to IP 1.1.1.3 with `dig foo.example.com`
6. If the attack didn't work, it might be because you have lost the race condition, goto `4.`
7. Notice that other hosts in the `example.com` domain aren't affected by the attack, e.g. `dig bar.example.com`

To perform the **Kaminsky attack**:

1. Restart the lab so that you start from a clean environment
2. On the <REDACTED> DNS's device, set delay with: `tc qdisc add dev eth0 root netem delay 1500ms`
3. Edit `./shared/kaminsky.cpp` with `vscode`: `code ./shared`
4. On the attacker's device, compile your code: `g++ -o kaminsky /shared/kaminsky.cpp -ltins`
5. On the attacker's device run the script: `./kaminsky`
6. On the victim's device, verify that example.com has ns at 1.1.1.254 with `dig example.com`. Every sub-domain should resolve to IP 1.1.1.3.

7. If the attack didn't work, it might be because you have lost the race condition, goto `5.`
8. Notice that this time, every host under `example.com` resolves to the attacker's IP address

Useful commands:

- stop the kathara lab (you will lose everything you have done so far): `kathara lclean`
- clear the cache of a DNS: `rndc flush`
- print the cache entries for *example.com*: `rndc dumpdb -cache && grep "example.com" /var/cache/bind/dump.db`
- edit the delay: `tc qdisc change dev eth0 root netem delay 2000ms`
- remove the delay: `tc qdisc del dev eth0 root netem delay 2000ms`

Browser inside the terminal:

- use `links` to start it;
- type `g` to start searching for a URL;
- type `q` to exit.