590B Assignment 3 Writeup

Aaron Kaplowitz - 11/20/16

Description

My script uses the DNS-hold on technique described in the paper we read in class last month. A single run works as follows, using the IP address of the provided testing DNS server:

1. First, send a DNS query for a non-sensitive website. Our testing server only attacks requests for `falun.com`, but I used a site that won't likely ever be censored by anybody - `m.pvta.com`, which is the mobile site of Western MA's public transit service. We record the RTT of the request/response and the TTL of the response.

2. Now that we have an expected RTT and TTL, we send a DNS lookup request for the hostname given as a param to the script (default to `falun.com`) to the testing server, which we know will trigger it to inject a response. We wait a configurable amount of time (default to 15 seconds), keeping the socket open for any potential response to our query. This is a key part of hold-on - a standard DNS implementation would simply return the first valid response it sees.

3. After the timer has run out, we look at each response we received. If the RTT is less than half of the expected RTT (which we recorded in step 1), we assume it was injected. If the testing server behaved like an actual attack server, we'd also check to see if the TTL of each response matched the TTL from step 1, and assume it's injected if they don't match. However, the testing server has a slightly different

implementation than hold-on expects, so we don't do the TTL check in my script and focus solely on the RTT.

Output

Testing server:

```
python dns-holdon.py -s 130.245.145.6 -n falun.com -t 15
```

```
An evil DNS resolver tried to lie and tell you that falun.com is at 130.245.145.6 but it's not!
```

```
falun.com is actually at 192.121.234.16
```

Using Chinese IP

I found the chinese IP by looking up autonomous systems that make up China's internet "border." From these, I researched which ASes are most known to do injections, both GFW and DNS. From those, I picked one and did some research into the most-used DNS servers run by each and performed some trial-and-error to determine an IP that would inject responses. In the end, I ended up choosing `222.73.128.165`, which is on `AS4812` (China Telecom). It's in a /24 that sits on the border and is a DNS resolver.

Instead of `falun.com`, it's a better idea to use `facebook.com`, which is well-known to be completely blocked inside of China. Here's the output:

```
python dns-holdon.py -s 222.73.128.165 -n facebook.com -t 15
```

```
An evil DNS resolver tried to lie and tell you that facebook.com is at 78.16.49.15 but it's not!
```

```
facebook.com is actually at 31.13.71.36
```