CSCI-UA.0480-063: Intro. to Security & Cryptography Fall 2025

Project 2: Network reconnaissance

due: Tuesday 2025-11-11 22:00 EDT via classes.nyu.edu

Note: You may discuss with fellow students but you must complete the assignment *on your own.*

In this project you'll explore the setup and security parameters of any THREE domains of your choosing which support HTTPS. Please choose a diverse set, preferably:

- One commercial domain (e.g. `google.com`, `chase.com`, `rei.com`)
- One non-profit domain (e.g. `eff.org`, `accessfund.org`, `bronxzoo.com`)
- One domain run by a government outside of the USA (e.g. `www.servicesaustralia.gov.au`, `www.interieur.gouv.fr`, `www.presidence.sn`)

You're encouraged to choose domains that are interesting to you personally.

For each of the three domains, answer the following questions. These questions rely on command-line tools you may have to install, commands are shown here as if you are analyzing www.`example.com`

1. **Domain registration.** First, lookup the official ownership information for this domain: `whois example.com`
    a. Who is the official registrant? Is it registered openly, privately, or by proxy?
    b. Do they provide a phone number? A physical address? Are these plausible?
    c. When was the domain created, and when is it registered until?
2. **DNS.** Resolve this domain's IP address using DNS: `dig +trace www.example.com ANY.`
    a. What is the domain's IP address?
    b. Querying this domain's IP address using iplocation.net, what city, latitude and longitude do you get?
    c. Which records are returned, besides A records?
    d. Does the domain have a mail server?
    e. Does it support DNSSEC?
3. **IP routing:** Check your IP path to this domain: `traceroute www.example.com`
    a. How many hops does the connection have?
    b. Did each packet take the same route?

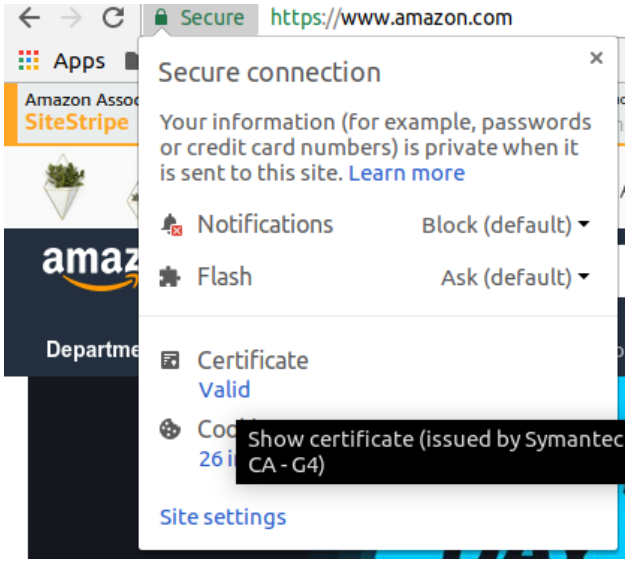
c. How many routers could be identified (i.e. they were not displayed as *)? The unidentified routers are either behind a firewall blocking ICMP pings or themselves refused to respond.

d. For the last identifiable router on the path-what geolocation is provided by iplocation.net?

4. **TCP.** Next, query for open ports at this domain: `nmap www.example.com`.

   a. Which ports are open and which services do they represent?

5. **PKI.** Connect to the domain's web site using your browser to inspect its certificate for HTTPS. The interface will vary slightly based on your browser, here it is for Chrome:



   a. Which ciphersuite did the site negotiate with your browser?

   b. What size and type of public key does the certificate include?

   c. When does the certificate expire and what is its total validity period?

   d. Which root Certificate Authority issued the site's certificate? What size and type of public key does the root CA use and when does it expire?

   e. Which other domains share this certificate?

   f. How many intermediate certificates are in the certificate chain (possibly zero)?

   g. Is the site using an extended validation certificate?

   h. Does the certificate include an OCSP responder? Does it include a CRL distribution point?

i. Look up the certificate (e.g. by its hash) in the Certificate Transparency search engine https://crt.sh. How many CT logs include this certificate? When was it first logged?

6. **TLS.** Finally, check the domain's Qualys SSL report card: (https://www.ssllabs.com/ssltest/)

   a. Which versions of TLS/SSL are supported?

   b. What is the server's most-preferred cipher suite? Does this provide forward secrecy?

   c. Did the server fail to complete a handshake with any of the clients simulated by Qualys?

   d. Does the server support Strict Transport Security (HSTS)? With what max-age?

   e. Finally-if the server received lower than an A grade, what caused it to lose points?

7. Tor and VPNs. Finally, install both NYU's supported VPN client and Tor Browser.

   a. Before using either of these tools, determine your IP address using https://2ip.io/. What is your IP? What geolocation and IP address did the site report? What result do you get if you pass this IP address through reverse DNS?

   b. Repeat the above, connecting via NYU's VPN and then via Tor.

   c. For your Tor IP address, also look it up at Tor's Relay Search. What is your Tor exit node's nickname? What uptime and bandwidth are reported? What other flags are reported for this node?

   d. Finally, reconnect to your three chosen domains via NYU's VPN and via Tor. Is access allowed? Do you notice any difference in the rendered sites?

8. **Wrap-up/comparison.** Finally, write a few sentences describing what you learned from investigating and analyzing your three chosen domains. What was surprising to you? How would you compare the overall security of these domains? What do you think explains the differences?