Assessing External SSL

By: Matt Molda

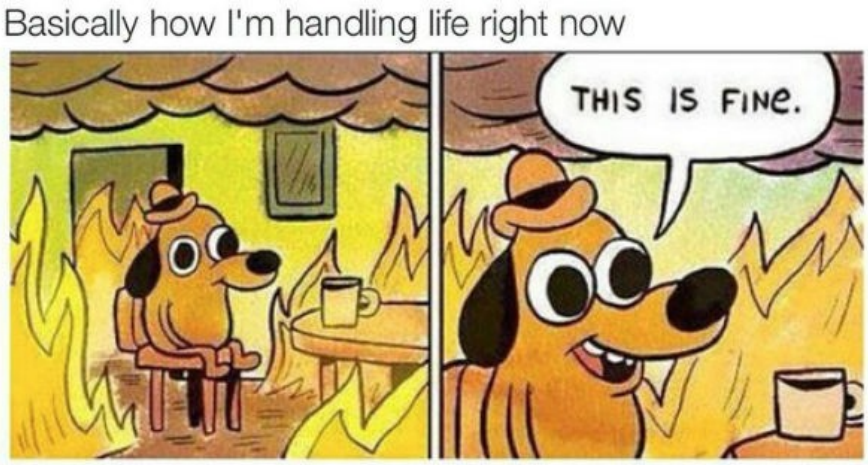
Disclaimer

While most of this information is publicly available some consider scanning or enumerate a domain not owned by you to be bad netiquette.

Some of these command can cause lots of traffic to systems. Use with care!

Why Check External SSL?

- Compliance
- Provides protections for customers
- Helps identify gaps in domain management practices. (Seems like most companies don’t know what all they have)
- Cause others can too...



SecMN
Minnesota Security Professionals

Identifying External Domains

- Identify external network range
  - Whois to CIDR Ranges
  - Any additional recon you want to do (Recon-ng)
- Identifying hosts
  - DNS Enumeration with Nmap
  - Passive DNS
  - Shodan?
  - DNS Dumpster
  - Subdomain brute forcing

SecMN
Minnesota Security Professionals

DNS Enumeration Nmap

- Given CIDR we can look for active DNS entries
- Probably don’t want to put load on your DNS servers so use google’s or someone else's.
- May not find all external hosts since it is only reverse lookup
- If no cache information exists your NS will be queried. Might want to implement a slower enumeration. -T3 or -T2

nmap --dns-servers 8.8.8.8,8.8.4.4 -sL CIDR

CAUTION

Passive DNS Enumeration

- DNSDB - Passive with API to https://www.dnsdb.info/ - Have to apply for service.
- DNS Dumpster
- If you subscribe to some Threat Intel Service like RiskIQ or others they may have this data also.

DNS Dumpster Sample

DNS Servers

ns4.domain.mn.	50.23.75.44 2c.4b.1732.ip4.static.sl-reverse.com	AS36351 SoftLayer Technologies Inc. United States
ns6.domain.mn.	184.173.150.58 3a.96.adb8.ip4.static.sl-reverse.com	AS36351 SoftLayer Technologies Inc. United States
ns3.domain.mn.	50.23.136.173 ad.88.1732.ip4.static.sl-reverse.com	AS36351 SoftLayer Technologies Inc. United States
ns5.domain.mn.	67.15.253.219 earth.orderbox-dns.com	AS21844 SoftLayer Technologies Inc. United States

MX Records ** This is where email for the domain goes...

0 smtp.secureserver.net.	68.178.213.203 p3plibsmtp03-v01.prod.phx3.secureserver.net	AS26496 GoDaddy.com, LLC United States
10 mailstore1.secureserver.net.	72.167.238.32 p3pismtp01-065.prod.phx3.secureserver.net	AS26496 GoDaddy.com, LLC United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

SecMN
Minnesota Security Professionals

DNS Enumeration Continued

- We have domains but don’t know what all ports web servers are ran on…
- Can run against default 443 or use DNMAP to scan known domains for other web servers and ports
- Might also want to check for subdomains. DNSRecon, Subbrute, Recon-ng

Qualys SSL Labs API

- performs the same function as the website
- can output into json for parsing
- takes host and port from file or individual server
- Finds common SSL issues
  - Beast
  - RC4
  - POODLE
  - FREAK
  - HeartBleed
  - Logjam
  - + more

Qualys SSL Labs API

- Can also report:
  - SSL Protocol versions supported (SSLv2/3,TLS1 to TLS1.2)
  - Negotiated Protocol based on client
  - Certificate Details (Chain, Issuer, Expiration Date, Strength, Algorithm)
  - Server Signatures
  - HSTS Information

Qualys SSL Labs API - Setup

- Download from GitHub
- Requires Go >=1.3

```
Usage of ./ssllabs-scan:
  -api="BUILTIN": API entry point, for example https://www.example.com/api/
  -grade=false: Output only the hostname: grade
  -hostcheck=false: If true, host resolution failure will result in a fatal error.
  -hostfile="": File containing hosts to scan (one per line)
  -ignore-mismatch=false: If true, certificate hostname mismatch does not stop assessment.
  -insecure=false: Skip certificate validation. For use in development only. Do not use.
  -json-flat=false: Output results in flattened JSON format
  -maxage=0: Maximum acceptable age of cached results, in hours. A zero value is ignored.
  -quiet=false: Disable status messages (logging)
  -usecache=false: If true, accept cached results (if available), else force live scan.
  -verbosity="info": Configure log verbosity: error, notice, info, debug, or trace.
  -version=false: Print version and API location information and exit
```

• Download from GitHub
• Requires Go >=1.3
• Compile Go App

Qualys SSL Labs Command

./ssllabs-scan --quiet=true --hostfile=mycompanydomains.txt --ignore-mismatch=true --hostcheck=false --usecache=false >> results.json

- to get the proper json output --quiet needs to be passed
- --ignore-mismatch means if the cert doesn’t match the name continue with the check
- --hostcheck=false means if host resolution fails it won’t stop the scan
- --usecache=false do not use the existing results if there but to do all the checks again

SSL Labs Json Output

<insert sample or show sample of json output here>

SSL Labs Parser

- python script
- parses json and outputs to xlsx for easy review
- includes most information returned, but not all
- customize for your needs

SSL Labs Parser Example

cat mycompanydomains.json |
./ssllabparser_toxlsx.py

- outputs to xlsx named SSLLabsScanResults_<date>_<time>.xlsx

SSL Labs Parser Example

ALEXA TOP 500

Links

https://github.com/g1ldedm1n1on/scripts - ssllabsparser_toxlsx.py
https://dnsdumpster.com
https://www.ssllabs.com/ssltest/
https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide.pdf