Practical Networking

Practical TLS – Lab Guide

A deep dive into SSL and TLS – the protocols that secure the Internet

Lab 5.1 – Cipher Suite Enumeration

In this lab you will discover all the Cipher Suites that are supported by various SSL websites. You will then use the knowledge you learned in this module to analyze the supported ciphers and create an overall opinion on the security posture of each website.

Create working directory and acquire lab files

1. Navigate to the folder you created in Lab 0.0 named Practical-TLS

   ```
   $ cd Practical-TLS
   ```

2. Create and navigate to a new directory for Lab 5.1 files:

   ```
   $ mkdir “LAB5.1 – Cipher Suite Enumeration”
   $ cd “LAB5.1 – Cipher Suite Enumeration”
   ```

3. There are no files to download for this lab. You will be creating files during the lab.

Lab Instructions

Select *(at least)* three websites which you browse to regularly. This could be a school or company website, a social media website, an e-mail website, or any other HTTPS enabled website.

Run the `nmap` script `ssl-enum-ciphers` for *each* of the websites and output the results to a text file. This will make it easier to review the output in the future without having to execute the script again.

Analyze the supported ciphers for each website to make a determination of each website’s general security posture. There are some reflection questions provided at the end of the lab steps below.

Enumerating SSL and TLS Ciphers

In the instructions below, replace every instance of **site.com** with the website you are testing.

1. Verify if you have the correct version of nmap which includes the ssl-enum-ciphers script:
    - `nmap  --script ssl-enum-ciphers  -p 443  site.com > site.com.txt`
    - The script will run for approximately 30 seconds up to two minutes.
    - When finished, you will have a new file in your directory: `site.com.txt`
2. Repeat the steps above for each website you have selected.
3. Examine the contents of your output files:
    - `cat site.com.txt`
    - `cat site.com.txt`
    - `cat site.com.txt`

    Replace each instance of site.com.txt with an output file from a website you analyzed.

4. Analyze the supported ciphers. Below are some questions that can help guide your thoughts:
    - What versions of SSL are supported?
    - How many ciphers are supported for each version of SSL?
    - How many ciphers are supported that are graded “A”, “B”, “C”, “D”, “E”, or “F” ?
    - Can you identify why ciphers graded C-F are graded as such?
    - Are there any ciphers that use a Key size less than 128 bits?
    - Are there any ciphers that use Export grade cryptography?
    - Which ciphers provide Forward Secrecy?
    - Which ciphers do not provide Forward Secrecy?
    - Did any website support a Null cipher?
    - Which ciphers were AEAD ciphers?
    - Overall, do you approve of the list of Cipher Suites each website has chosen to support?

OPTIONAL – Testing Additional Sites with Peculiar Ciphers

After completing the steps above for at least three websites of your choosing, you may optionally consider running the same test against the following lists of websites which have known weak ciphers:

- `null.badssl.com`
- `dh512.badssl.com`
- `rc4.badssl.com`
- `rc4-md5.badssl.com`
- `3des.badssl.com`
- `cbc.badssl.com`

Additionally, if you come across any other interesting findings when performing these tests, please share them in the Discord server and discuss the results with other students.