Practical Networking

Practical TLS – Lab Guide

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

Lab 4.1 – Certificate Chains

In this lab you'll get to work with Certificate Chains. In each task below, you will be provided with a set of Certificates and you'll have to sort them into their proper chain. **There are three tasks**: the first task is easier to get you warmed up to working with Certificate chains. The second and third tasks are progressively more challenging to reflect what you might encounter in the real world.

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 a new directory for Lab 4.1 files:
   - `$ mkdir “LAB4.1 – Certificate Chains”`

3. Download *one* of the following lab files and place it in the newly created folder:
   - `LAB 4.1 Files - Certificate Chains - Practical TLS.tar.gz`
   - `LAB 4.1 Files - Certificate Chains - Practical TLS.zip`

   The lab files are in `.zip` or `.tar.gz` format – the contents within are identical, use whichever file is easier for you

4. Unzip or Untar the file you downloaded into your LAB 4.1 working directory:
   - For the TAR.GZ file, you will use the Linux command: `tar -xvzf “LAB 4.1 ...`
   - For the ZIP file, it should be something like right clicking the file and selecting “Extract All…”

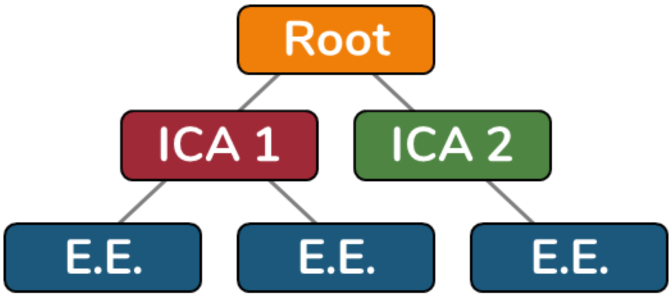
5. When finished, you should have the following three directories and 23 files (total):

```
./Task1/:
brown.net.cert  cyan.net.cert  magenta.net.cert  olive.net.cert  yellow.net.cert

./Task2/:
batman.com.cert    ironman.com.cert   professorX.com.cert   spiderman.com.cert
superman.com.cert  thor.com.cert      wolverine.com.cert    wonder.woman.com.cert

./Task3/:
apocalypse.com.cert    dark.phoenix.com.cert    loki.com.cert     psylocke.com.cert
ultron.com.cert        bane.com.cert            joker.com.cert    magneto.com.cert
thanos.com.cert        venom.com.cert
```

Map out the full Certificate Chain of every certificate in each Directory

The lab files contain three directories: **Task1** **Task2** **Task3**

In each directory are many different certificate files. Your task is to map out the files in their proper certificate chain order. You'll draw out something like this:



The box on top will be the Root CA certificate. And each box below represents whatever certificate(s) that Root CA has signed. This will continue until the boxes at the bottom which represent the End Entity certificates.

The certificates in Task1 start off relatively easy, with all certificates belonging to a single chain. The certificates in Task2 and Task3 become progressively more difficult.

The commands you learned in LAB 3.1 will help you complete these tasks. Particularly the commands you learned in the last task of LAB 3.1.

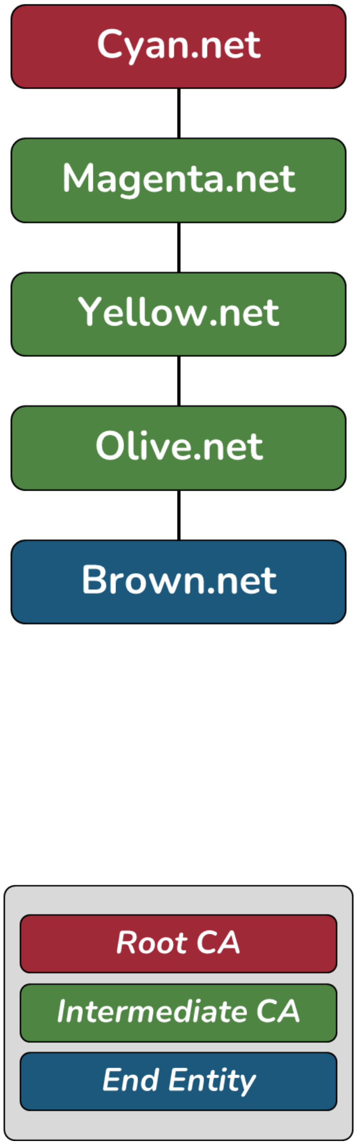
This page intentionally left blank

Answers for the tasks above are on the next page.

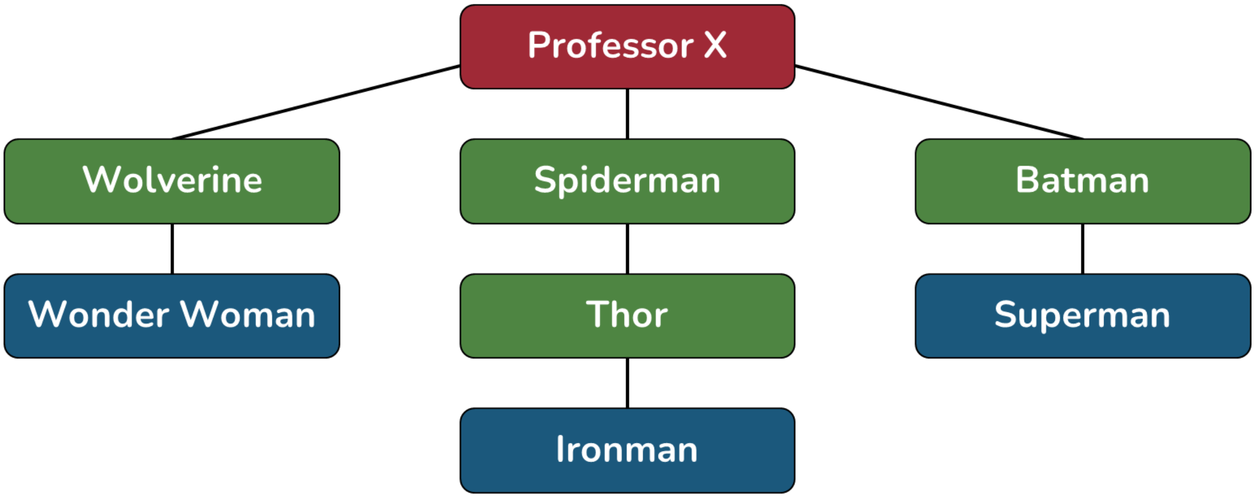
Complete the tasks then check your answers against the answers below

If you are unclear about a question and answer, ask about it in the Discord server.

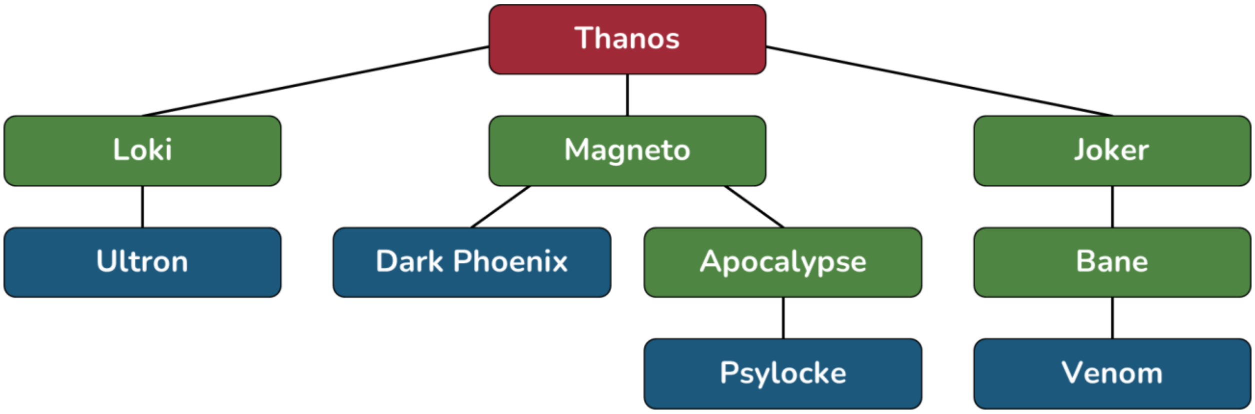
Answer Key – Task 1



Answer Key – Task 2



Answer Key – Task 3


Thanos
Loki
Magneto
Joker
Ultron
Dark Phoenix
Apocalypse
Bane
Psylocke
Venom