Introduction

A customer asks you to analyze and assess various aspects of the security of its infrastructure with regard to certificates. Record your findings on all aspects in a written report.

Remember to check the integrity of the files in the resource section after downloading by calculating and comparing the MD5 checksum.

```
MD5 (c8-certificates_scan_report-task-3.csv) = 7dcd80ae068cbb4503303a37c99fc755
```

```
MD5 (c8-certificates-task-4.zip) = add2be6534c5e70a3f4c968d1991ed78
```

Goal and tasks

Task 1

Launch and scan the host in the RESOURCE section for ports with certificates. List all ports with certificates in your report and provide evidence for your findings.

Task 2

Select a port with a certificate on the host, and perform with suitable commands an in-depth analysis of the security at this port. Indicate the selected port in your report and record the output of your commands. Analyze the results and propose in your report exactly 3 measures to improve security at the selected port.

Task 3

The CSV file in the resource section contains the results of a certificate scan of a DNS zone of the customer. Examine the given list for insecure certificates.

List in your report the serial numbers of all certificates in the list that cannot be considered secure in a business context. Provide for each identified certificate the reasons for your assessment.

Task 4

The ZIP file in the resource section contains the certificates of the chain

```
Root            Intermediate            End Entity
root-ca.pem ==> intermediate-ca.pem ==> cert.pem
```

as well as the certificate bundle file chain.pem.

Verify with openssl the CRL revocation status of the end entity certificate and all certificates in the chain. Hint: Verify each certificate separately.

Record the commands and outputs in your report. Analyze the results and explain in your report whether the end entity certificate can be considered as valid or not. Submission

Submit a written report as PDF document, containing your results and findings as well as all details on how you retrieved the information.