Challenge #8
Analyze certificates

Anchoring and overview

Modul:	681	Angriffe auf ICT-Infrastrukturen detektieren und abwehren
Handlungsziele:	HZ 2	Wählt geeignete Überwachungs- und Schutzlösungen zur netzwerkbasierten Erkennung und Abwehr von Angriffen aus und nimmt diese in Betrieb.
Leistungskriterien PO:	LK-B-3	CSS können geeignete Verfahren und Werkzeuge für die Überwachung von Systemen auszuwählen und einzusetzen
	LK-B-5	CSS können Protokollierungen von unterschiedlichen Systemen und in unterschiedlichen Formaten auswerten und interpretieren

Formulation of task (candidate view)

Analyze certificates

Resources

[1] Docker of host to be scanned in tasks 1 & 2
[2] Scan report as CSV file to be analyzed in task 3
`c8-certificates_scan_report-task-3.csv` - MD5-Checksum: xxx
[3] ZIP file containing certificates to be analyzed in task 4
`c8-certificates_task-4.zip` - MD5-Checksum: xxx

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.

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.

Specifications for correction

Evaluation criteria

Task 1

C01: All ports with certificates listed correctly	= 1 pt.
C02: Approach documented, traceable and evidence included	= 1 pt.

Task 2

C03: In-depth analysis for selected port done and documented	= 1 pt.
C04: Measure #1 proposed, specific and technically correct	= 1 pt.
C05: Measure #2 proposed, specific and technically correct	= 1 pt.
C06: Measure #3 proposed, specific and technically correct	= 1 pt.

Task 3

C07: A minimum of 2 certificates correctly identified and justified	= 1 pt.
C08: 3 or 4 certificates correctly identified and justified	= 1 pt.
C09: 5 or 6 certificates correctly identified and justified	= 1 pt.
C10: 7 certificates correctly identified and justified	= 1 pt.
C11: 8 certificates correctly identified and justified	= 1 pt.

Task 4

C12: Verification of root certificate documented and traceable	= 1 pt.
C13: Verification of intermediate certificate documented and traceable	= 1 pt.
C14: Verification of end entity certificate documented and traceable	= 1 pt.
C15: Conclusion available and technically correct	= 1 pt.

Correction instructions

- This challenge gives a maximum of **15 points**.
- Given scores on the criteria may not be further subdivided.
- Task 2: If the solution contains more than 3 measures, only the first 3 will be scored.
- Task 3: A justification with all reasons is expected in addition to the identification of the certificate. Correctly listed certificates **without** justification do not give points. Wrong listed identified certificates are ignored during correction.

Sample solutions

Task 1

Solution: List of ports with certificates:

- Port **443**
- Port **6000**
- Port **8443**
- Port **8444**
- Port **21021**
- [Port 22] → Specifying port 22 is optional, since some tools (i.e., nmap) recognize this port even though a key pair is used instead of a certificate.

Possible approach: Scanning the host with **`nmap`**

```
nmap -sS -p1-65535 --script ssl-cert $HOST
```

or

```
nmap -sS -sC -p1-65535 $HOST
```

```
┌──(seb㉿RT-QLS-NBK-016)-[/tmp/os]
└─$ sudo nmap -sS -sC -p1-65535 $HOST
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 15:42 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   2048 6f:f7:91:26:d3:b3:41:78:1b:a0:ac:92:2c:29:bb:e7 (RSA)
|   256 c9:d0:03:0c:07:01:ce:d7:0d:26:61:d2:66:c1:7d:af (ECDSA)
|_  256 d3:5d:8f:63:71:69:ab:42:a1:37:cd:3e:9d:21:5f:c9 (ED25519)
80/tcp    open  http
443/tcp   open  https
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=www.mycompany.local/organizationName=MyCompany/countryName=CH
| Subject Alternative Name: DNS:domain
| Not valid before: 2022-08-01T13:32:52
|_Not valid after:  2023-08-01T13:32:52
|_http-title: Site doesn't have a title (text/html).
999/tcp   open  garcon
3128/tcp  open  squid-http
3390/tcp  open  dsc
4949/tcp  open  munin
6000/tcp  open  X11
| ssl-cert: Subject: commonName=ws.mycompany.local/organizationName=MyCompany/countryName=CH
| Subject Alternative Name: DNS:domain
| Not valid before: 2022-08-01T13:32:52
|_Not valid after:  2023-08-01T13:32:52
|_ssl-date: TLS randomness does not represent time
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
| ssl-cert: Subject: commonName=tomcat-int.mycompany.local/organizationName=MyCompany/countryName=CH
| Subject Alternative Name: DNS:domain
| Not valid before: 2022-08-01T13:32:52
|_Not valid after:  2023-08-01T13:32:52
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (text/html).
8444/tcp  open  pcsync-http
| ssl-cert: Subject: commonName=tomcat-dev.mycompany.local/organizationName=MyCompany/countryName=CH
| Subject Alternative Name: DNS:domain
| Not valid before: 2022-08-01T13:32:52
|_Not valid after:  2023-08-01T13:32:52
|_ssl-date: TLS randomness does not represent time
21021/tcp open  unknown
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=portal-dev.mycompany.local/organizationName=MyCompany/countryName=CH
| Subject Alternative Name: DNS:domain
| Not valid before: 2022-08-01T13:32:52
|_Not valid after:  2023-08-01T13:32:52

Nmap done: 1 IP address (1 host up) scanned in 3.70 seconds
```

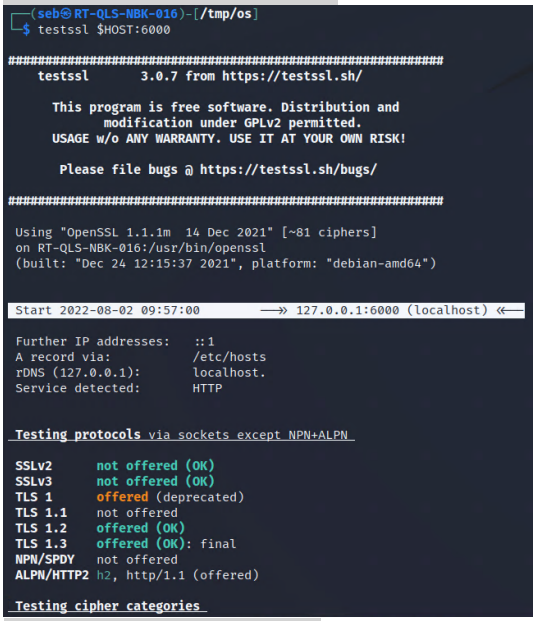
Task 2

Solution: The following measures apply to all ports and are therefore independent of the selection of the applicant:

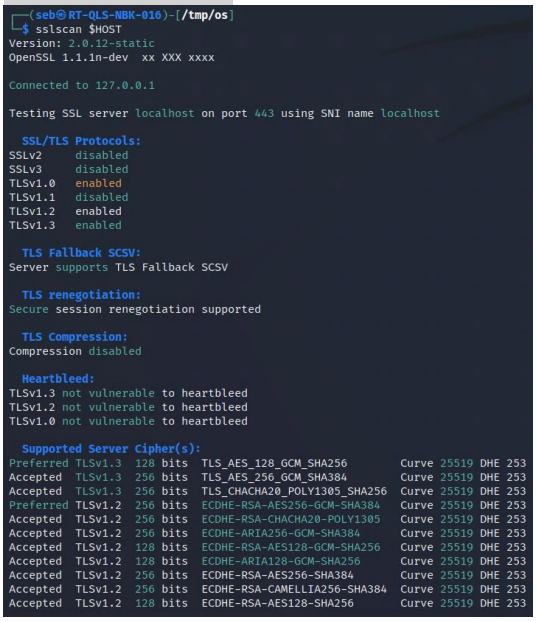
- Replace certificate (public certificate or at least add CRL/OCSP information to internal certificate)
- Disable TLS 1.0
- Enforce server cipher order
- Disable weak ciphers (e.g., CBC ciphers)
- Implement HTTP Strict Transport Security (HSTS)
- Remove server header information (server_tokens nginx directive)

Possible approach: Various commands can be used, but the most common are the following:

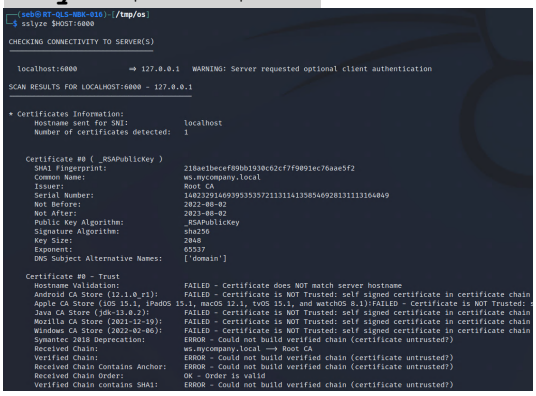
testssl $HOST:$PORT



sslscan $HOST



sslyze $HOST:$PORT



Task 3

#	**Certificate** DNS Name	**Reason(s)**
1	5aa4a0918ad1e4da595fdae59f7caa0984d72d34 sintswab.mycorp-machine.com	• Expired
2	d4b550bac3121a75e9a80d7673c4b00 trunkd-mycorp-acceptance.apps.emea.phapps.io	• Wildcard
3	1b0834f455a1a1728e05ffdb9ec5d277f46a31bc rd.swabcd.mycorp-machine.com	• SelfSigned
4	47857bbeb5e2025a6f47d37a4b58712ae9a prelive.nc.mycorp-connect.com	• Untrusted Authority (Let's Encrypt)
5	a45f4798640c48090be1005823ceb46 approval.cba.mycorp-connect.com	• Missmatch DNS/CA
6	767a2243928293c143d614c3c27f4d8002f9fb3f dev2swab.mycorp-machine.com	• Revoked
7	22000057f780dacbab7fc0848a0001000057f7 sodp-swab-4a.mycorp-machine.com	• NO CRL / NO OCSP / Private CA
8	7a1231d6d4622cb82ff62eceb8f56571900f69d1 shop.mycorp-connect.com	• Unsecure algorithm / standard (SHA12) and weak key (RSA1024)

Task 4

Step #1: Verification of Root CA certificate `root_ca.pem`. Hint: No CRL revocation must be done since a Root CA is self-signed and has no CRL for itself):

```
openssl verify -verbose -CAfile chain.pem root_ca.pem
```

```
┌──(seb㉿RT-QLS-NBK-016)-[~]
└─$ openssl verify -verbose -CAfile chain.pem root_ca.pem
root_ca.pem: OK
```

Step #2: Verification of Intermediate CA certificate `intermediate_ca.pem`:

```
openssl verify -crl_download -crl_check -verbose -CAfile chain.pem intermediate_ca.pem
```

```
┌──(seb㉿RT-QLS-NBK-016)-[~]
└─$ openssl verify -crl_download -crl_check -verbose -CAfile chain.pem intermediate_ca.pem
C = CH, O = FISlab, CN = FISlab ICT Issuing CA 2022 G2
error 23 at 0 depth lookup: certificate revoked
error intermediate_ca.pem: verification failed
```

Step #3: Verification of end entity certificate:

```
openssl verify -crl_download -crl_check -verbose -CAfile chain.pem cert.pem
```

```
┌──(seb㉿RT-QLS-NBK-016)-[~]
└─$ openssl verify -crl_download -crl_check -verbose -CAfile chain.pem cert.pem
cert.pem: OK
```

Conclusion: The end entity certificate itself is not revoked by the Intermediate CA, but the Intermediate CA was revoked by the Root CA. Therefore, this certificate should be considered as **not valid**.

Background: openssl parameters:

- `-crl_download`: attempts to download CRL information for the certificate. If omitted, openssl will display a "unable to get certificate CRL" error message.
- `-crl_check`: checks end entity certificate validity by attempting to look up a valid CRL. If a valid CRL cannot be found an error occurs. If omitted, no CRL check will be attempted.
- `-CAfile`: a file of trusted certificates. The file contains the whole CA chain in PEM format concatenated together (Root + Issuing CA). If omitted, openssl cannot construct the chain and will display a "unable to get local issuer certificate" error message.