Mikołaj Piotrowski - raport; Zadanie 2

Zadanie/cele:

Zadanie 2: (kontynuacja zadania 1)
1. Proszę przygotować dwa certyfikaty klienckie dla certyfikatu serwera z Zadania 1 p.1 - `User A`, `User B`
2. Ścieżka `/only-user-a` (wraz ze wszystkimi podścieżkami) ma być dostępna wyłącznie dla klientów z certyfikatem `User A`
3. Ścieżka `/only-user-b` (wraz ze wszystkimi podścieżkami) ma być dostępna wyłącznie dla klientów z certyfikatem `User B`
4. Ścieżka `/user-a-or-b` (wraz ze wszystkimi podścieżkami) ma być dostępna wyłącznie dla klientów z certyfikatem `User A` lub `User B`
5. (punkt dodatkowy, nieobowiązkowy) Podścieżka `/info` dla ścieżek z p. 2,3,4 (czyli np. `/only-user-a/info`) wyświetli informacje o użytkowniku odczytane z jego certyfikatu klienckiego

Tworzenie certyfikatów dla Apache i Nginx

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx]
└─$ mkdir ssl

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx]
└─$ ls
apache  docker-compose.yml  nginx  site  site2  ssl
```

Apache

1. certyfikaty pośrednie (CA)

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl req -newkey rsa:2048 -nodes -keyform PEM -keyout apache-ca.key -x509 -days 3650
outform PEM -out apache-ca.crt

[sudo] password for kali:
Generating a RSA private key
.............+++++
.............+++++
writing new private key to 'apache-ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Dol
Locality Name (eg, city) []:WRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWR
Organizational Unit Name (eg, section) []:W04
Common Name (e.g. server FQDN or YOUR name) []:my-apache.com
Email Address []:mik@pio.com
```

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl genrsa -out apache.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................+++++
.....................................................................................
.....................+++++
e is 65537 (0×010001)

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl req -new -key apache.key -out apache.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Dol
Locality Name (eg, city) []:WRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWR
Organizational Unit Name (eg, section) []:W04
Common Name (e.g. server FQDN or YOUR name) []:my-apache.com
Email Address []:mik@pio.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl x509 -req -in apache.csr -CA apache-ca.crt -CAkey apache-ca.key -set_serial 100 -day
s 365 -outform PEM -out apache.crt

Signature ok
subject=C = PL, ST = Dol, L = WRO, O = PWR, OU = W04, CN = my-apache.com, emailAddress = mik@pio.com
Getting CA Private Key
```

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ ls
apache-ca.crt  apache-ca.key  apache.crt  apache.csr  apache.key
```

2. klucze

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl genrsa -out apache-userA.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................+++++
.....................................+++++
e is 65537 (0×010001)

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl genrsa -out apache-userB.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
........+++++
....+++++
e is 65537 (0×010001)
```

3. certyfikaty

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl req -new -key apache-userA.key -out apache-userA.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Dol
Locality Name (eg, city) []:WRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWR
Organizational Unit Name (eg, section) []:W04
Common Name (e.g. server FQDN or YOUR name) []:userA
Email Address []:user@A.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:A
string is too short, it needs to be at least 4 bytes long
A challenge password []:userA
An optional company name []:userA
```

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl req -new -key apache-userB.key -out apache-userB.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Dol
Locality Name (eg, city) []:WRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWR
Organizational Unit Name (eg, section) []:W04
Common Name (e.g. server FQDN or YOUR name) []:userB
Email Address []:user@B.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:userB
An optional company name []:userB
```

4. Podpisanie certyfikatów

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl x509 -req -in apache-userA.csr -CA apache-ca.crt -CAkey apache-ca.key -set_serial 10
1 -days 365 -outform PEM -out apache-userA.crt

[sudo] password for kali:
Signature ok
subject=C = PL, ST = Dol, L = WRO, O = PWR, OU = W04, CN = userA, emailAddress = user@A.com
Getting CA Private Key

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl x509 -req -in apache-userB.csr -CA apache-ca.crt -CAkey apache-ca.key -set_serial 10
1 -days 365 -outform PEM -out apache-userB.crt

Signature ok
subject=C = PL, ST = Dol, L = WRO, O = PWR, OU = W04, CN = userB, emailAddress = user@B.com
Getting CA Private Key
```

5. Stworzenie zestawów klucz+certyfikat

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl pkcs12 -export -inkey apache-userA.key -in apache-userA.crt -out apache-userA.p12

Enter Export Password:
Verifying - Enter Export Password:

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ ls
apache-ca.crt  apache.csr        apache-userA.csr  apache-userB.crt  nginx-ca.crt  nginx.csr
apache-ca.key  apache.key        apache-userA.key  apache-userB.csr  nginx-ca.key  nginx.key
apache.crt     apache-userA.crt  apache-userA.p12  apache-userB.key  nginx.crt

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl pkcs12 -export -inkey apache-userB.key -in apache-userB.crt -out apache-userB.p12

Enter Export Password:
Verifying - Enter Export Password:

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ ls
apache-ca.crt  apache.csr        apache-userA.csr  apache-userB.crt  apache-userB.p12  nginx.crt
apache-ca.key  apache.key        apache-userA.key  apache-userB.csr  nginx-ca.crt      nginx.csr
apache.crt     apache-userA.crt  apache-userA.p12  apache-userB.key  nginx-ca.key      nginx.key

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$
```

Nginx

6. certyfikaty pośrednie (CA)

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl req -newkey rsa:2048 -nodes -keyform PEM -keyout nginx-ca.key -x509 -days 3650    -o
utform PEM -out nginx-ca.crt

Generating a RSA private key
.....................................................+++++
.............................+++++
writing new private key to 'nginx-ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Dol
Locality Name (eg, city) []:WRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWR
Organizational Unit Name (eg, section) []:W04
Common Name (e.g. server FQDN or YOUR name) []:my-nginx.com
Email Address []:mik@pio.com
```

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl genrsa -out nginx.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................+++++
.........................+++++
e is 65537 (0×010001)

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl req -new -key nginx.key -out nginx.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Dol
Locality Name (eg, city) []:WRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWR
Organizational Unit Name (eg, section) []:W04
Common Name (e.g. server FQDN or YOUR name) []:my-nginx.com
Email Address []:mik@pio.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl x509 -req -in nginx.csr -CA nginx-ca.crt -CAkey nginx-ca.key -set_serial 110 -days 3
65 -outform PEM -out nginx.crt

Signature ok
subject=C = PL, ST = Dol, L = WRO, O = PWR, OU = W04, CN = my-nginx.com, emailAddress = mik@pio.com
Getting CA Private Key
```

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ ls
apache-ca.crt  apache.crt  apache.key  nginx-ca.key  nginx.csr
apache-ca.key  apache.csr  nginx-ca.crt  nginx.crt  nginx.key
```

7. klucze

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl genrsa -out nginx-userA.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................+++++
.............................+++++
e is 65537 (0×010001)

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl genrsa -out nginx-userB.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.................................+++++
.....................................................................+++++
e is 65537 (0×010001)
```

8. certyfikaty

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl req -new -key nginx-userA.key -out nginx-userA.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Dol
Locality Name (eg, city) []:WRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWR
Organizational Unit Name (eg, section) []:W04
Common Name (e.g. server FQDN or YOUR name) []:userA
Email Address []:user@A.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:userA
An optional company name []:userA
```

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ openssl req -new -key nginx-userB.key -out nginx-userB.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Dol
Locality Name (eg, city) []:WRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWR
Organizational Unit Name (eg, section) []:W04
Common Name (e.g. server FQDN or YOUR name) []:userB
Email Address []:user@B.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:userB
An optional company name []:userB
```

9. Podpisanie certyfikatów

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl x509 -req -in nginx-userA.csr -CA nginx-ca.crt -CAkey nginx-ca.key -set_serial 111 -
days 365 -outform PEM -out nginx-userA.crt

Signature ok
subject=C = PL, ST = Dol, L = WRO, O = PWR, OU = W04, CN = userA, emailAddress = user@A.com
Getting CA Private Key

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl x509 -req -in nginx-userB.csr -CA nginx-ca.crt -CAkey nginx-ca.key -set_serial 112 -
days 365 -outform PEM -out nginx-userB.crt

Signature ok
subject=C = PL, ST = Dol, L = WRO, O = PWR, OU = W04, CN = userB, emailAddress = user@B.com
Getting CA Private Key
```

10. Stworzenie zestawów klucz+certyfikat

```
┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl pkcs12 -export -inkey nginx-userA.key -in nginx-userA.crt -out nginx-userA.p12

Enter Export Password:
Verifying - Enter Export Password:

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ sudo openssl pkcs12 -export -inkey nginx-userB.key -in nginx-userB.crt -out nginx-userB.p12

Enter Export Password:
Verifying - Enter Export Password:

┌──(kali㉿kali)-[~/Desktop/BAW-NGINX-APACHE-strona/ssl-docker-nginx/ssl]
└─$ ls
apache-ca.crt  apache-userA.crt  apache-userB.csr  nginx.crt        nginx-userA.key  nginx-userB.p12
apache-ca.key  apache-userA.csr  apache-userB.key  nginx.csr        nginx-userA.p12
apache.crt     apache-userA.key  apache-userB.p12  nginx.key        nginx-userB.crt
apache.csr     apache-userA.p12  nginx-ca.crt      nginx-userA.crt  nginx-userB.csr
apache.key     apache-userB.crt  nginx-ca.key      nginx-userA.csr  nginx-userB.key
```

Implementacja certyfikatów dla Apache i Nginx

11. Skonfigurowano docker-compose.yml tak by przekazywał nowopowstałe certyfikaty do serwerów

```
services:
  server1:
    image: nginx:latest
    volumes:
      - ./nginx/nginx.conf:/etc/nginx/nginx.conf
      - ./site:/usr/share/nginx/html
      - ./ssl/nginx.crt:/etc/nginx/ssl/my-nginx.com.pem
      - ./ssl/nginx.key:/etc/nginx/ssl/my-nginx.com.key
      - ./ssl/nginx-ca.crt:/etc/nginx/ssl/nginx-ca.pem
      - ./ssl/nginx-userA.crt:/etc/nginx/ssl/userA.crt
      - ./ssl/nginx-userB.crt:/etc/nginx/ssl/userB.crt
    ports:
    - "8080:80"
    - "8443:443"
```

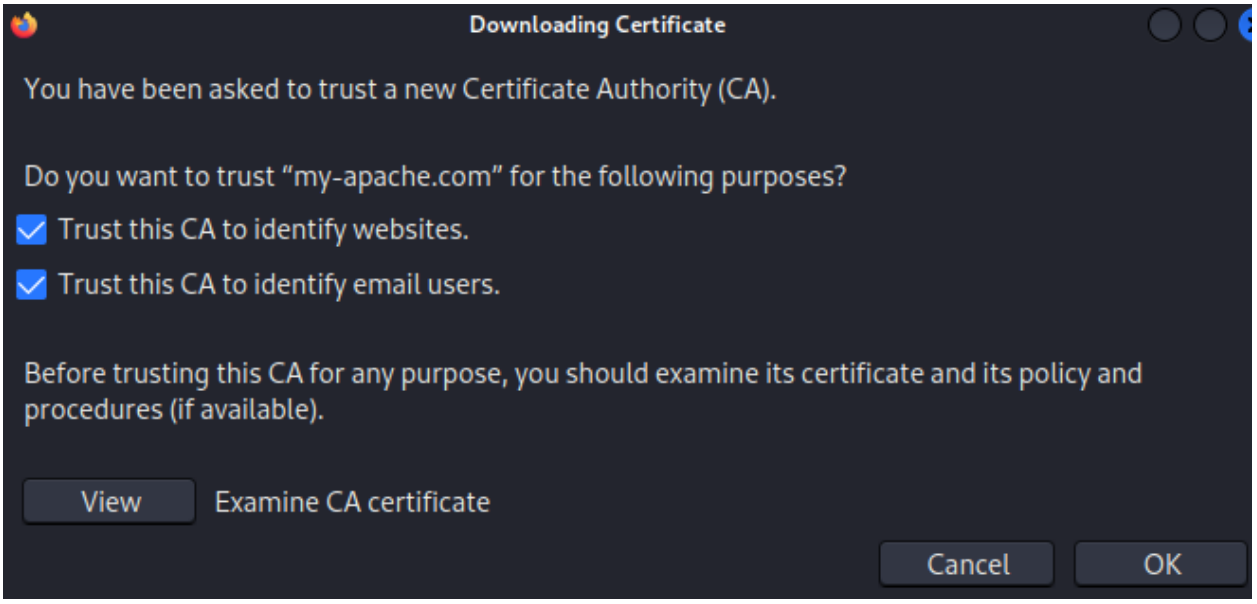
```
server2:
  image: httpd:latest
  ports:
  - "80:80"
  - "443:443"
  volumes:
    - ./apache/httpd.conf:/usr/local/apache2/conf/httpd.conf
    - ./site2:/usr/local/apache2/htdocs
    - ./apache/httpd-ssl.conf:/usr/local/apache2/conf/extra/httpd-ssl.conf
    - ./ssl/apache.crt:/usr/local/apache2/conf/server.crt
    - ./ssl/apache.key:/usr/local/apache2/conf/server.key
    - ./ssl/apache-ca.crt:/usr/local/apache2/conf/apache-ca.crt
```

12. Skonfigurowano httpd-ssl.conf

```
#SSLCACertificatePath "/usr/local/apache2/conf/ssl.crt"
SSLCACertificateFile "/usr/local/apache2/conf/apache-ca.crt"
```

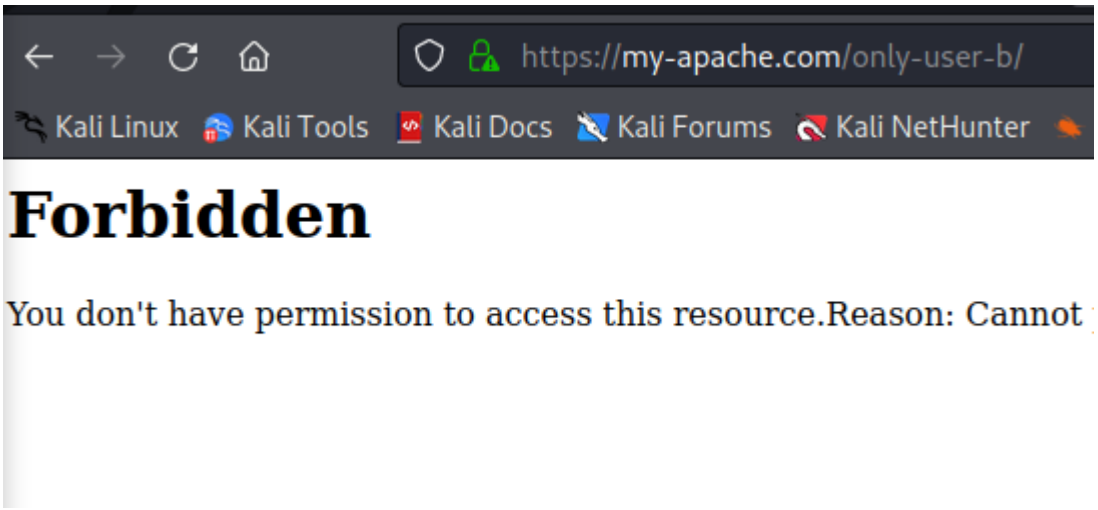
```
<Location /only-user-a/>
  SSLVerifyClient require
  SSLVerifyDepth  10
  SSLRequire %{SSL_CLIENT_S_DN_CN} eq "userA"
</Location>

<Location /only-user-b/>
  SSLVerifyClient require
  SSLVerifyDepth  10
  SSLRequire %{SSL_CLIENT_S_DN_CN} eq "userB"
</Location>

<Location /user-a-or-b/>
  SSLVerifyClient require
  SSLVerifyDepth  10
  SSLRequire %{SSL_CLIENT_S_DN_CN} in {"userA", "userB"}
</Location>
```

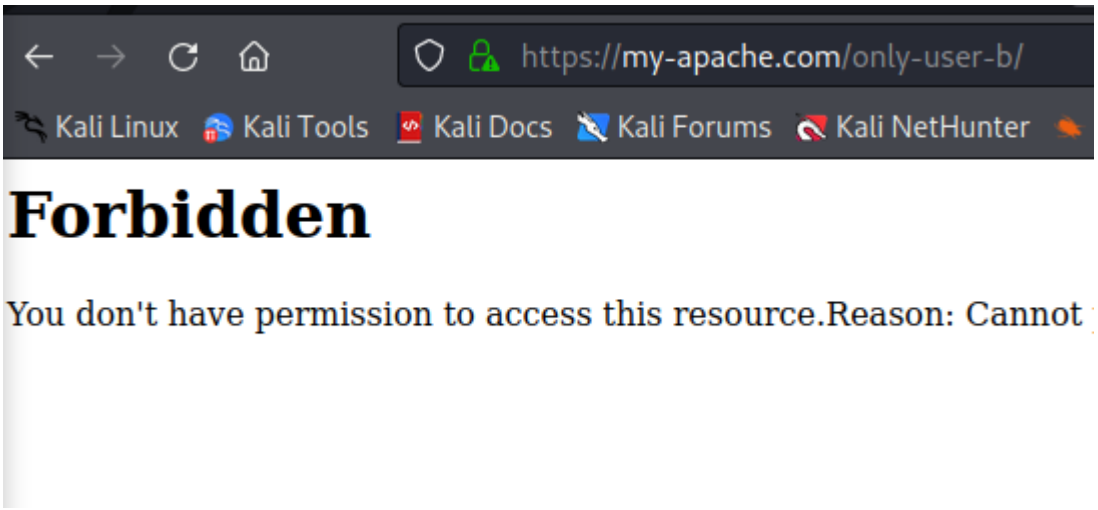
13. Dodano certyfikaty do przeglądarki

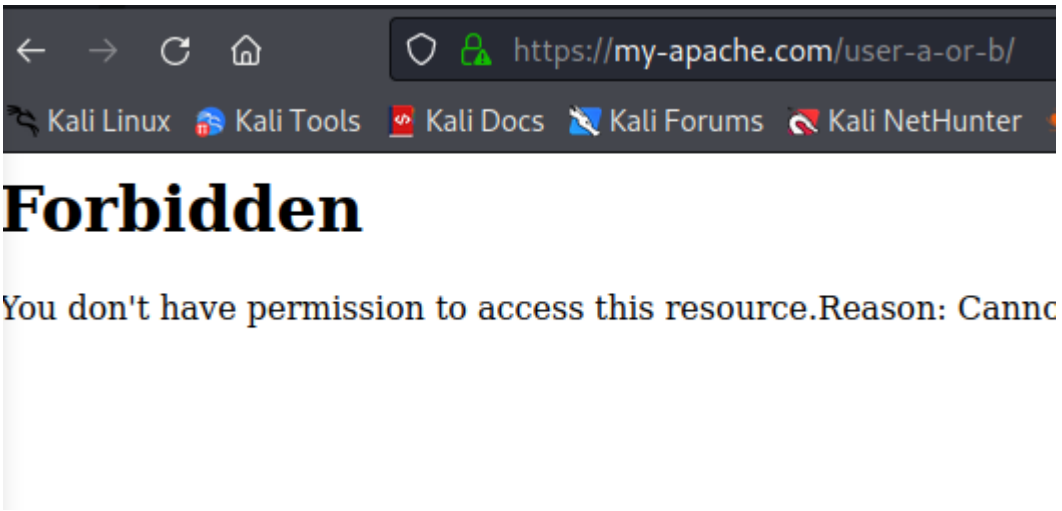


Testowanie certyfikatów dla Apache

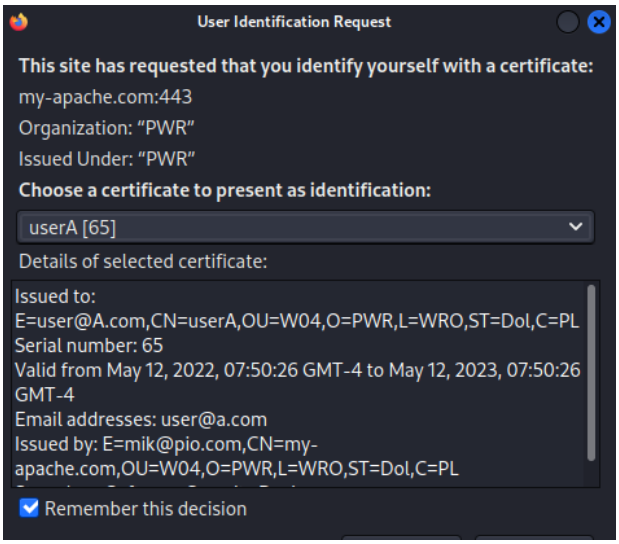
14. Bez certyfikatu

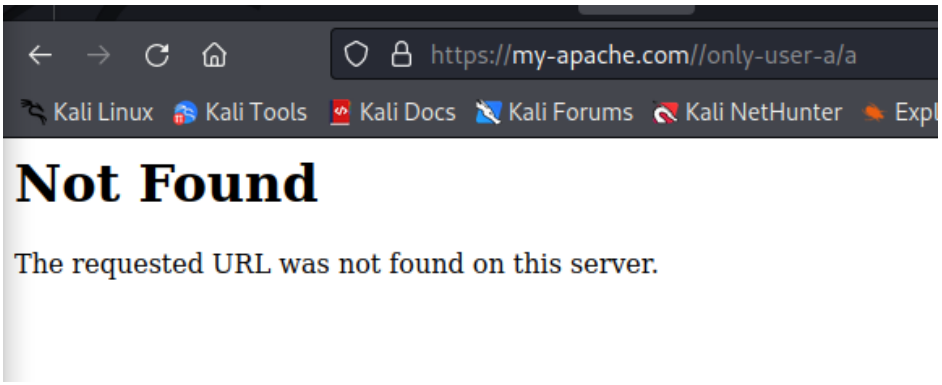


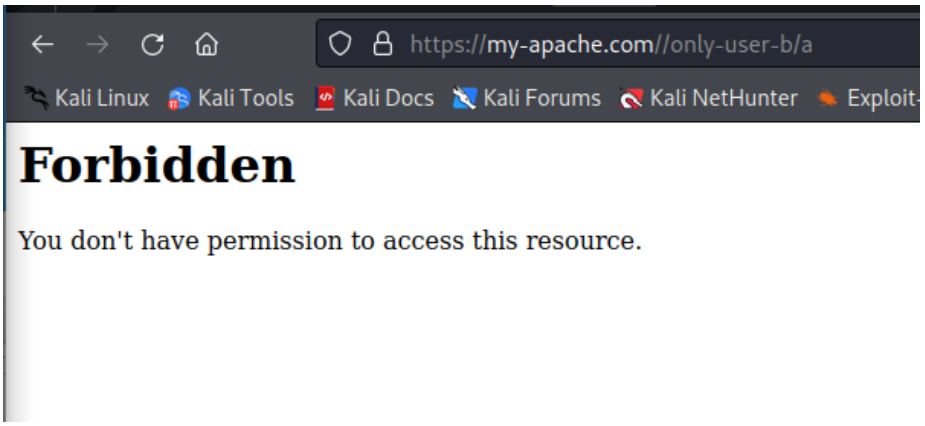


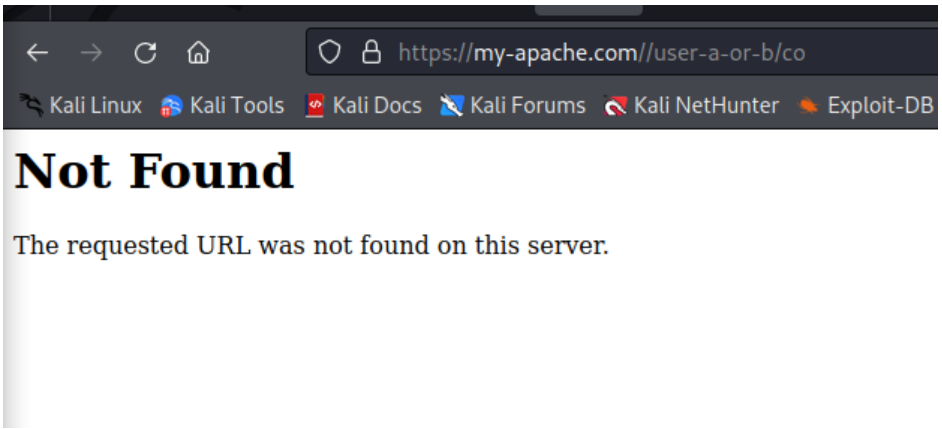


15. Z certyfikatem A









16. Z certyfikatem B