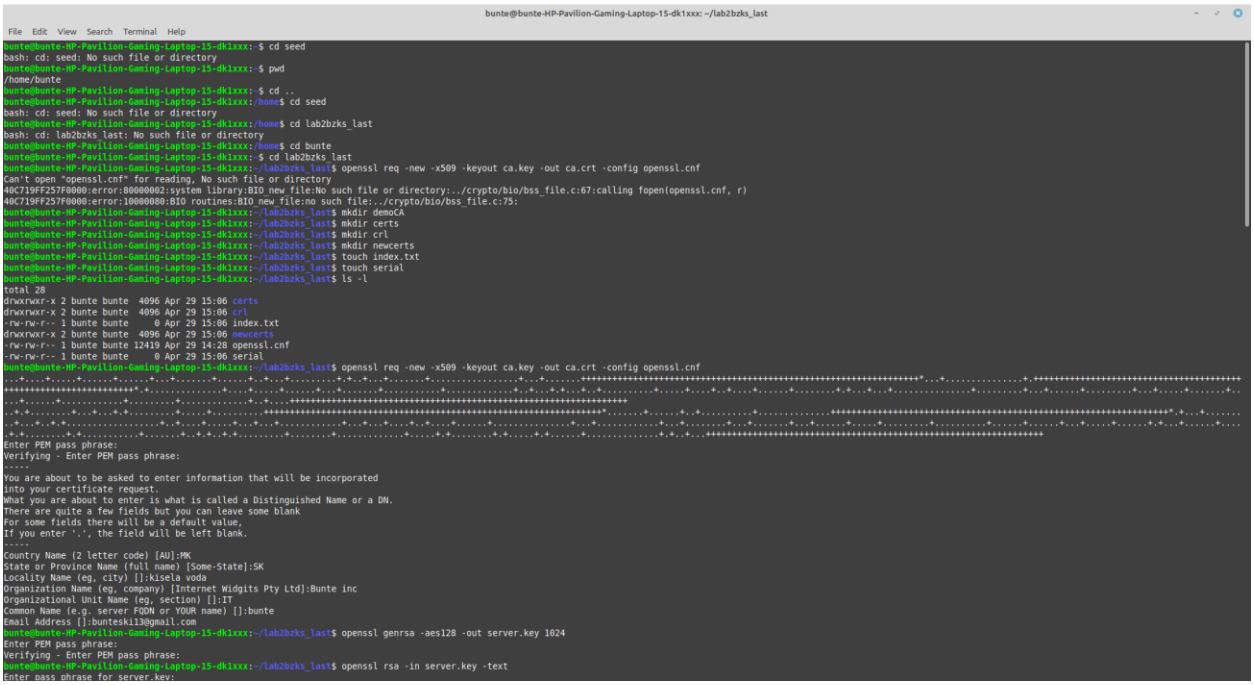
Лабораториска вежба бр.2

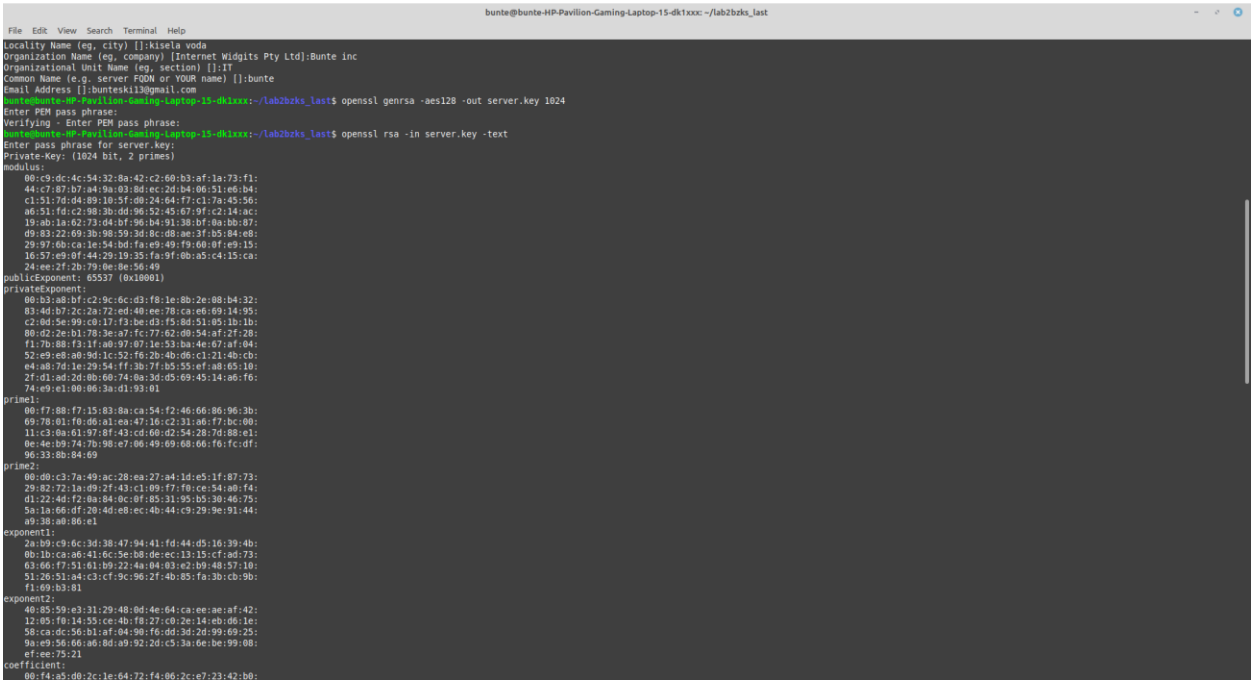
Инфраструктура на јавен клуч

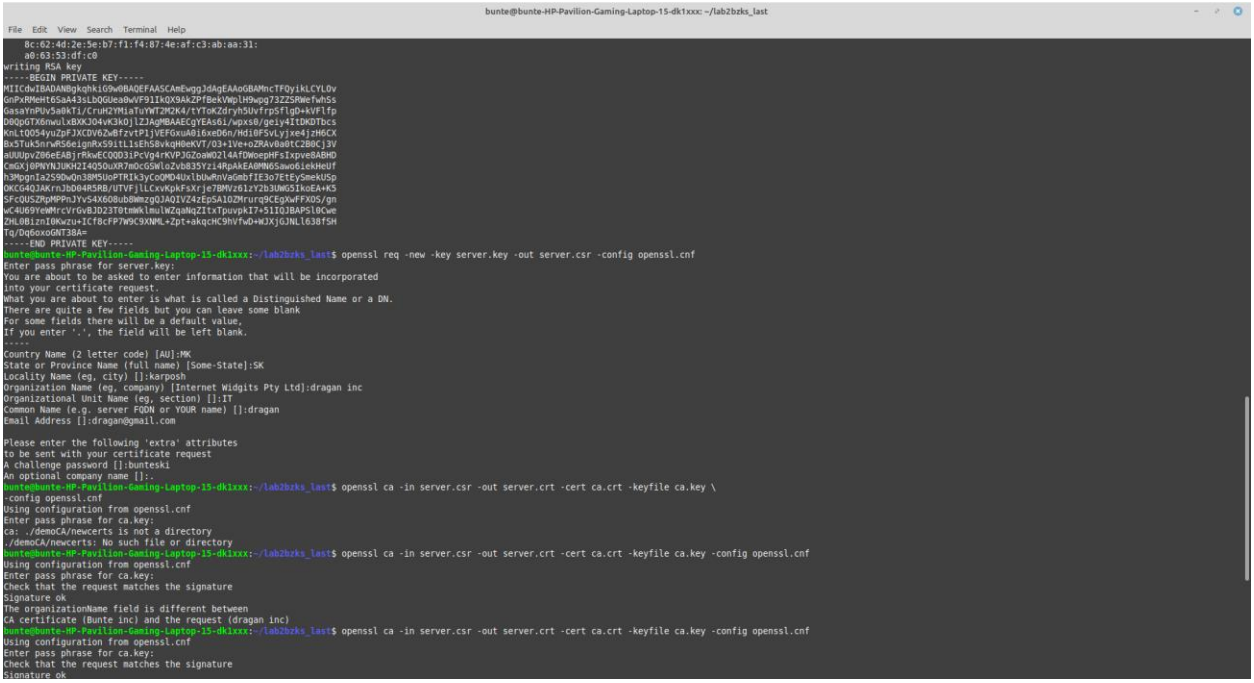
Марко Бунтески 129/2021

1. zadaca



2. zadaca

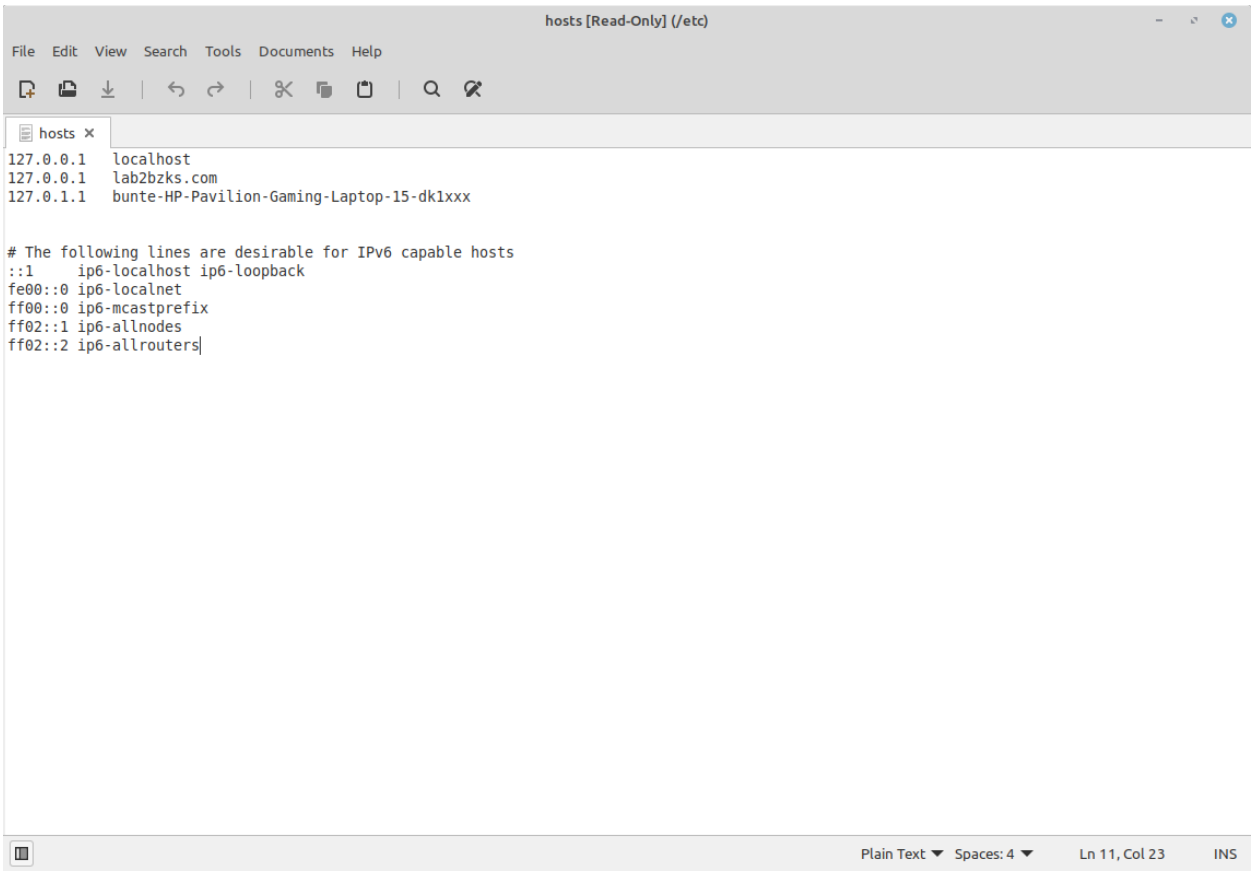


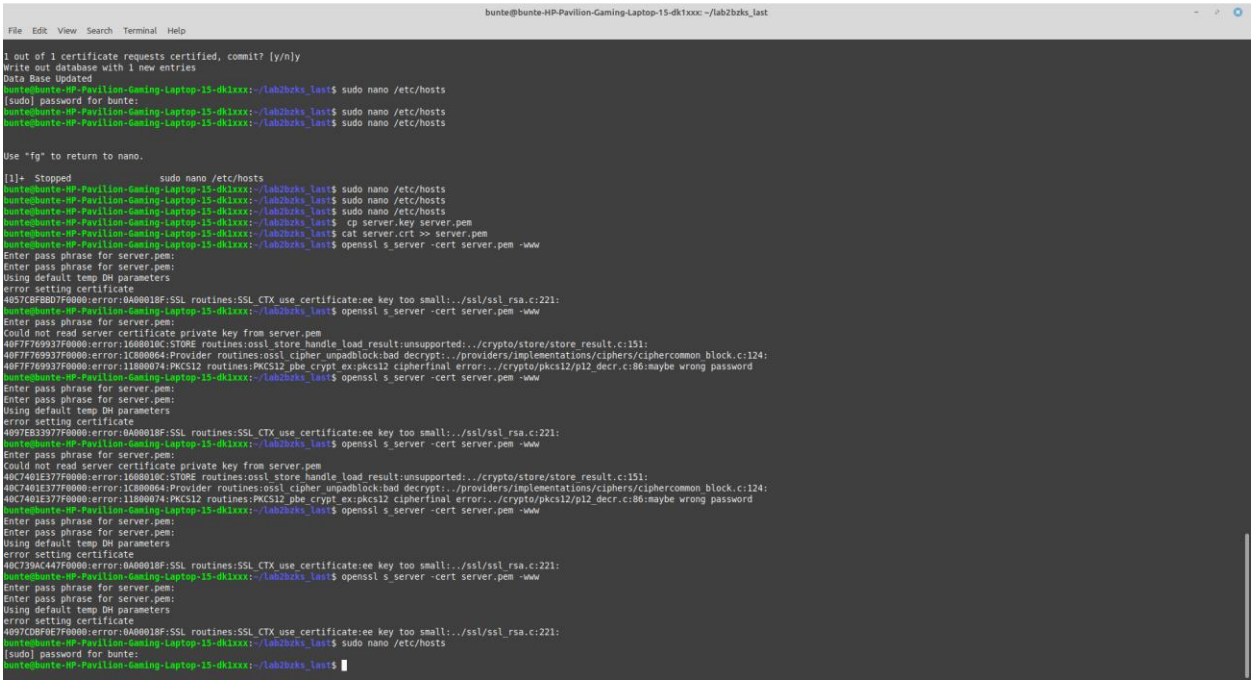

bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last
File Edit View Search Terminal Help
8c:62:4d:2e:5e:b7:f1:f4:87:4e:af:c3:ab:aa:31:
a0:63:53:df:c0
writing RSA key
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAMncTFQyikLCYLOv
GnPxRNeH6SaA43sLbQGUea0vVF91IkOX9AkZPfBekVWplH9wpg73ZZSRWefwhSs
GasaYnPUv5a0kTi/CruH2YMiaTuYWT2M2K4/tYToKZdryh5UvfrpSflgD+kVFlfp
D0QpGTX6nwulxBXKJO4vK3kOjlZJAgMBAAECgYEAs6i/wpxs0/geiy4ItDKDTbcs
KnLtQO54yuZpFJXCDV6ZwBfzvtP1jVEFGxuA0i6xeD6n/Hdi0FSvLyjxe4jzH6CX
Bx5TukSnrwRS6eignRxS9itL1sEhS8vkqH0eKVT/O3+1Ve+oZRAv0a0tC2B0Cj3V
mU0UpvZ0GEEABjrRkwECOQD3iPcVg4rKVPJGZoaWO2l4AfDWoepHFsIqveBABHQ
CmGKj0PNYNJUKH2I4Q5OuXR7mOcGSWloZvb835Yzi4RpAkEA0MN6Sawo6iekHeUf
h3MpgnIa2S9DwQn38M5UoPTRIk3yCoQMD4UxlbUwRnVaGmbfIE3o7EtEySmekUSp
OKCG4QJAKrnJbD04R5RB/UTVFjlLCxvKpkFsXrje7BMVz61zY2b3UWG5IkoEA+K5
SFcQUS2KpMPPnJYvS4X6OBubBWmzgQJAQ1VZ4zEpSA1OZMrurq9CEgXwFFXOS/gn
wC4U69YeMYcVYGvBJQ23T0tmWklmuWZqaNqZItxTpuvpkI7+51IQJBAPS10Cwm
ZHL0Bizn10Kwzu+ICf8cFP7W9C9XNML+Zpt+akqcHC9hVfwD+WJXjGJNLl638fSH
Tq/Dq6oxoGNT38A=
-----END PRIVATE KEY-----
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.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]:MK
State or Province Name (full name) [Some-State]:SK
Locality Name (eg, city) []:karposh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:dragan inc
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:dragan
Email Address []:dragan@gmail.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:bunteski
An optional company name []:.
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key \
-config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
ca: ./demoCA/newcerts is not a directory
./demoCA/newcerts: No such file or directory
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The organizationName field is different between
CA certificate (Bunte inc) and the request (dragan inc)
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok


bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last
File Edit View Search Terminal Help
State or Province Name (full name) [Some-State]:SK
Locality Name (eg, city) []:karposh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:dragan inc
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:dragan
Email Address []:dragan@gmail.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:bunteski
An optional company name []:.
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key \
-config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
ca: ./demoCA/newcerts is not a directory
./demoCA/newcerts: No such file or directory
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The organizationName field is different between
CA certificate (Bunte inc) and the request (dragan inc)
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number: 4096 (0x1000)
Validity
Not Before: Apr 29 13:19:46 2024 GMT
Not After : Apr 29 13:19:46 2025 GMT
Subject:
countryName = MK
stateOrProvinceName = SK
localityName = karposh
organizationName = dragan inc
organizationalUnitName = IT
commonName = dragan
emailAddress = dragan@gmail.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
72:18:8A:2C:6B:59:BE:8A:0F:AA:19:5D:93:6D:7A:17:09:4F:08:7C
X509v3 Authority Key Identifier:
14:66:27:CC:37:5F:DE:34:FD:15:E1:5A:27:56:74:A8:74:8C:7F:8F
Certificate is to be certified until Apr 29 13:19:46 2025 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$

3.


hosts [Read-Only] (/etc)
File Edit View Search Tools Documents Help
hosts
127.0.0.1 localhost
127.0.0.1 lab2bzks.com
127.0.1.1 bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx
The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
Plain Text
Spaces: 4
Ln 11, Col 23
INS


bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx: ~/lab2bzks_last
File Edit View Search Terminal Help
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ sudo nano /etc/hosts
[sudo] password for bunte:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ sudo nano /etc/hosts
Use "fg" to return to nano.
[1]+ Stopped sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ sudo nano /etc/hosts
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ cp server.key server.pem
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ cat server.crt >> server.pem
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
error setting certificate
4057CBFB8D7F0000:error:0A00018F:SSL routines:SSL_CTX_use_certificate:ee key too small:../ssl/ssl_rsa.c:221:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Could not read server certificate private key from server.pem
40F7F769937F0000:error:1608010C:STORE routines:ossl_store_handle_load_result:unsupported:../crypto/store/store_result.c:151:
40F7F769937F0000:error:1C800064:Provider routines:ossl_cipher_unpadblock:bad decrypt:../providers/implementations/ciphers/ciphercommon_block.c:124:
40F7F769937F0000:error:11800074:PKCS12 routines:PKCS12_pbe_crypt_ex:pkcs12 cipherfinal error:../crypto/pkcs12/p12_decr.c:86:maybe wrong password
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
error setting certificate
4097EB33977F0000:error:0A00018F:SSL routines:SSL_CTX_use_certificate:ee key too small:../ssl/ssl_rsa.c:221:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Could not read server certificate private key from server.pem
40C7401E377F0000:error:1608010C:STORE routines:ossl_store_handle_load_result:unsupported:../crypto/store/store_result.c:151:
40C7401E377F0000:error:1C800064:Provider routines:ossl_cipher_unpadblock:bad decrypt:../providers/implementations/ciphers/ciphercommon_block.c:124:
40C7401E377F0000:error:11800074:PKCS12 routines:PKCS12_pbe_crypt_ex:pkcs12 cipherfinal error:../crypto/pkcs12/p12_decr.c:86:maybe wrong password
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
error setting certificate
40C739AC447F0000:error:0A00018F:SSL routines:SSL_CTX_use_certificate:ee key too small:../ssl/ssl_rsa.c:221:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
error setting certificate
4097CDBF0E7F0000:error:0A00018F:SSL routines:SSL_CTX_use_certificate:ee key too small:../ssl/ssl_rsa.c:221:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$ sudo nano /etc/hosts
[sudo] password for bunte:
bunte@bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx:~/lab2bzks_last$

hosts [Read-Only] (/etc)

File Edit View Search Tools Documents Help

hosts

```
127.0.0.1   localhost
127.0.0.1   SEEDPKILab2018.com
127.0.1.1   bunte-HP-Pavilion-Gaming-Laptop-15-dk1xxx

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Plain Text Spaces: 4 Ln 11, Col 23 INS