

Lab Assignment 7

AP21110010302

Krish Srivastava

CSE – E

Network Security – CSE 315L

```
[retr0@parrot]~[/easy-rsa-3.0.1/easyrsa3]
$ sudo apt install strongswan-pki libcharon-extra-plugins libcharon-extauth-plugins libstrongswan-extra-plugins
[sudo] password for retr0:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
strongswan is already the newest version (5.9.8-5+deb12u1).
strongswan set to manually installed.
libcharon-extauth-plugins is already the newest version (5.9.8-5+deb12u1).
libcharon-extauth-plugins set to manually installed.
The following NEW packages will be installed:
  libcharon-extra-plugins libstrongswan-extra-plugins strongswan-pki
0 upgraded, 3 newly installed, 0 to remove and 107 not upgraded.
Need to get 687 kB of archives.
After this operation, 2,216 kB of additional disk space will be used.
Do you want to continue? [Y/n] yu
Get:1 https://deb.parrot.sh/parrot lory/main amd64 libcharon-extra-plugins amd64 5.9.8-5+deb12u1 [273 kB]
Get:2 https://deb.parrot.sh/parrot lory/main amd64 libstrongswan-extra-plugins amd64 5.9.8-5+deb12u1 [270 kB]
Get:3 https://deb.parrot.sh/parrot lory/main amd64 strongswan-pki amd64 5.9.8-5+deb12u1 [144 kB]
Fetched 687 kB in 2s (455 kB/s)
Selecting previously unselected package libcharon-extra-plugins.
(Reading database ... 525498 files and directories currently installed.)
Preparing to unpack .../libcharon-extra-plugins_5.9.8-5+deb12u1_amd64.deb ...
Unpacking libcharon-extra-plugins (5.9.8-5+deb12u1) ...
Selecting previously unselected package libstrongswan-extra-plugins.
Preparing to unpack .../libstrongswan-extra-plugins_5.9.8-5+deb12u1_amd64.deb ...
Unpacking libstrongswan-extra-plugins (5.9.8-5+deb12u1) ...
Selecting previously unselected package strongswan-pki.
Preparing to unpack .../strongswan-pki_5.9.8-5+deb12u1_amd64.deb ...
Unpacking strongswan-pki (5.9.8-5+deb12u1)
```

```
[retr0@parrot]~[/easy-rsa-3.0.1/easyrsa3]
$ pki --gen --type rsa --size 4096 --outform pem > ~/pki/private/ca-key.pem
'[retr0@parrot]~[/easy-rsa-3.0.1/easyrsa3]
$ [[200~pki --self --ca --lifetime 3650 --in ~/pki/private/ca-key.pem \
> --type rsa --dn "CN=VPN root CA" --outform pem > ~/pki/cacerts/ca-cert.pem
bash: '$'\E[200~pki': command not found
[x]-[retr0@parrot]~[/easy-rsa-3.0.1/easyrsa3]
$ pki --self --ca --lifetime 3650 --in ~/pki/private/ca-key.pem \
--type rsa --dn "CN=VPN root CA" --outform pem > ~/pki/cacerts/ca-cert.pem
[retr0@parrot]~[/easy-rsa-3.0.1/easyrsa3]
$ sudo mv /etc/ipsec.conf{,.original}
[retr0@parrot]~[/easy-rsa-3.0.1/easyrsa3]
$ sudo nano /etc/ipsec.conf
[retr0@parrot]~[/easy-rsa-3.0.1/easyrsa3]
$ sudo nano /etc/ipsec.secrets#
```

```
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo systemctl restart strongswan-starter
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo ufw enable
Firewall is active and enabled on system startup
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo ufw allow 500,4500/udp
Rule added
Rule added (v6)
```

```
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo ufw enable
Firewall is active and enabled on system startup
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo ufw allow 500,4500/udp
Rule added
Rule added (v6)
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $ip route show default
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo nano /etc/ufw/before.rules
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo nano /etc/ufw/sysctl.conf
[retr0@parrot]-[~/easy-rsa-3.0.1/easyrsa3]
└─ $sudo ufw disable
Firewall stopped and disabled on system startup
```



```

-----BEGIN CERTIFICATE-----
MIIDUTCCAjmGAWIBAgIUPJXzZ93MMzRyvJ6Dw7CWBOZDqZQwDQYJKoZIhvcNAQEL
BQAwGDEWMBQGA1UEAwNa3Jpc2hob3N0bmFtZTAeFw0yNDAzMzExNzI2NDhaFw0z
NDZMjYxNzI2NDhaMBGxGjAUBGNVBAMMDWtyaXNoaG9zdG5hbWUwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDLJ5Sx4qHpFTce47SE6mCJbNutUASp5lPv
dsxQztgN3EiRvmrGakdtST8ohpPNg9eF04ruayFb0aVzVP2pTq0tHiEoDkrARaSc
3HBfIcbIQWe5wLU8Rh6jlcVvwgyMzIHggXQLErzgy5WACPjuoGvsllJZnB2D44Yi
UC/nKxncf0mnn53wVoj4uKAjAtcqiz9VKVWtcx+AFkR2DbfmJoWADu2iIzefTKX3
G8fKiitWfFMC0HP77kCy9GWQjSW429oRuT26vhOSwedfSK65TPqSEajNNATHsfSD
9X00f4Km/oojjaUgCbpWhfrkNQshIvamrcOzgKS+VKEQ+MLbT39XAgMBAAGjgZIw
gY8wHQYDVIR0BBYEFPFYUBXgWbUF3gDXtLNSmmPgY6KcMFMGA1UdIwRMMEqAFPFY
UBXgWbUF3gDXtLNSmmPgY6KcMFMGA1UdIwRMMEqAFPFYUBXgWbUF3gDXtLNSmmPg
Y6KcMFMGA1UdIwRMMEqAFPFYUBXgWbUF3gDXtLNSmmPgY6KcMFMGA1UdIwRMMEqAFPFY
ghQ8lfnN3cwzNHK8noPDsJYE5k0pLDAMBGNVHRMEBTADAQH/MASGA1UdDwQEAwIB
BjANBgkqhkiG9w0BAQsFAAOCAQEAYVHT0yPhWxsZzaqjy3CLREcsJV20nEWRVHIV
QddK7xH4myR/Ck2T0hEZrn94tg10sik3Wb8zhTc4iwJE+7NRG2ZXDUooZQpW5fio
tCS4WbAfAtrWyXa7grjZcLLgHXP2v27X95kAAhq4ChahdjL5IuC95Y+b0jgV2/BM
COAXhjVWxZauSWuaf+ji+pANQ2pd4MxZg2tYu79Q0/mD54IxRlgo6cha6jiJB+Z
kmbY8lXd2oUF0HxVEPOXY1yV50iS0o8lhvrowgLq7EeSYVGiksShcIJfJiHD0F7N
rC8pZ+tlNLiR58hR1zF2tHP9eKB36W5nRy6gw1nNNyhILI3Qiw==
-----END CERTIFICATE-----

```

Configuring into windows:

```

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
>> -CertStoreLocation cert:\LocalMachine\Root\
>> -FilePath C:\lab7_ca-cert.pem

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\Root

Thumbprint                               Subject
-----
FB7D94D035DEAA4BE9A939F7E5C350781DB15F2A  CN=VPN root CA

```

```

PS C:\WINDOWS\system32> Add-VpnConnection -Name "VPN Connection"
>> -ServerAddress 192.168.25.2
>> -TunnelType "IKEv2"
>> -AuthenticationMethod "EAP"
>> -EncryptionLevel "Maximum"
>> -RememberCredential

```

```

PS C:\WINDOWS\system32> Get-VpnConnection -Name "VPN Connection"

Name                               : VPN Connection
ServerAddress                     : 192.168.16.1
AllUserConnection                 : False
Guid                              : {ED6D5235-78E9-4563-B662-94A9A6DB9FEB}
TunnelType                       : Automatic
AuthenticationMethod              : {Eap, MsChapv2}
EncryptionLevel                  : Optional
L2tpIPsecAuth                   : Certificate
UseWinlogonCredential            : False
EapConfigXmlStream               :
ConnectionStatus                 : Disconnected
RememberCredential               : True
SplitTunneling                   : False
DnsSuffix                        :
IdleDisconnectSeconds            : 0

```

```
PS C:\WINDOWS\system32> Set-VpnConnectionIPsecConfiguration -Name "VPN Connection"
>> -AuthenticationTransformConstants GCMAES256
>> -CipherTransformConstants GCMAES256
>> -DHGroup ECP384
>> -IntegrityCheckMethod SHA384
>> -PfsGroup ECP384
>> -EncryptionMethod GCMAES256

Confirm
Changing the Cryptography Settings. Do you want to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\WINDOWS\system32>
```