Script 1: This script provides a step-by-step method to create, import, and enable an SSL certificate for a brand-new Microsoft Exchange Server 2019. When Exchange is first installed, it uses a self-signed certificate so services can run immediately. Using this script, you can generate a Certificate Signing Request (CSR) for your domain (in this case, sstraining.online) to submit to a Certificate Authority (CA) and receive a signed certificate. After obtaining the signed certificate, you import it into Exchange. To enable it for services such as IIS, SMTP, IMAP, and POP, you need to use the certificate's thumbprint, which must be retrieved manually from the Exchange Management Shell and replaced in the script before running it. Finally, you run IISReset to apply the certificate to web services like OWA and Outlook Anywhere. This script guides the deployment process but requires the user to manually provide the thumbprint to activate the certificate correctly.

Create CSR Sample:

```
$txtrequest = New-ExchangeCertificate -GenerateRequest -SubjectName
"c=US,o=Certificate by SS,cn=mail.sstraining.online" -DomainName
mail.sstraining.online,autodiscover.sstraining.online


[System.IO.File]::WriteAllBytes('\\mail\cert\exchangecert.req',
[System.Text.Encoding]::Unicode.GetBytes($txtrequest))
```

Import Certificate Sample:

```
$cert = Import-ExchangeCertificate -FileData
([System.IO.File]::ReadAllBytes("\\Mail\Cert\certnew.cer")) -Password (Get-
Credential).password
```

Enable Certificate Sample:

```
Enable-ExchangeCertificate -Thumbprint -Services "IIS"
```

Example: Enable-ExchangeCertificate -Thumbprint 2548917C09385842A78C36F164425E611C72E541 -Services "IIS"

Run: IISReset command to restart Webservices

Script 2: This is a second script that you can use for the Exchange certificate. You can use either the first or second certificate, and both will give the same output.

 # 1. Generate CSR

```
New-ExchangeCertificate -GenerateRequest `
   -SubjectName "C=US,O=SSTraining,CN=MailServer.SSTraining.online" `
   -DomainName
autodiscover.SSTraining.online,mail.SSTraining.online,MailServer.SSTraining.online `
   -PrivateKeyExportable $true `
   -GenerateRequestFile "\\MailServer\Certs\Certreq.req"
```

 # 2. Import signed certificate

```
$cert = Import-ExchangeCertificate -Server "MailServer" -FileData
([System.IO.File]::ReadAllBytes("\\MailServer\Certs\Exchangecert.cer")) -
PrivateKeyExportable $true
```

 # 3. Enable certificate for IIS (replace thumbprint with actual thumbprint number)

```
Enable-ExchangeCertificate -Server "MailServer" -Thumbprint $cert.Thumbprint -Services
IIS
```

Example: Enable-ExchangeCertificate -Server "MailServer" -Thumbprint 2548917C09385842A78C36F164425E611C72E541 $cert.Thumbprint -Services IIS

 # 4. Restart IIS to apply the certificate

```
IISReset
```

Script 2 Explanation in Detail:

Domain Name: sstraining.online

Exchange Server Name: MailServer

The New-ExchangeCertificate -GenerateRequest command creates a certificate request for the Exchange server.

SubjectName: C=US,O=SSTraining,CN=MailServer.sstraining.online

- C=US → Country (United States)
- O=SSTraining → Organization name
- CN=MailServer.sstraining.online → Common Name (Exchange)

-DomainName: autodiscover.sstraining.online, mail.sstraining.online, MailServer.sstraining.online

- autodiscover.sstraining.online → Automatic email setup

- mail.sstraining.online → Mail server subdomain

- MailServer.sstraining.online → Main Exchange server

The request is saved using [System.IO.File]::WriteAllBytes to \\MailServer\Certs\Certreq.req and encoded in Unicode using [System.Text.Encoding]::Unicode.GetBytes($txtrequest).

Summary:

- Generates a certificate request for SSTraining covering all listed domains.
- Saves the request file Certreq.req in \\MailServer\Certs to send to a Certificate Authority.
- Prepares a certificate to secure all services and domains under sstraining.online, with MailServer as the Exchange server.