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