

Ejercicios de seguridad: realizar una comunicación UDP segura (utilizando Cryptographic Message Syntax)

Información

Enviar mensajes UDP

- <https://www.jesusninoc.com/01/23/enviar-varios-mensajes-entre-un-cliente-y-un-servidor-utilizando-el-mismo-canal-de-comunicacion-por-udp-en-powershell/>

Cifrar un mensaje con Cryptographic Message Syntax (CMS) usando certificados

- <https://www.jesusninoc.com/11/18/exports-a-certificate-to-a-personal-information-exchange-pfx-file/>

Importar un certificado para descifrar un mensaje cifrado con Cryptographic Message Syntax (CMS)

- <https://www.jesusninoc.com/11/20/imports-certificates-and-private-keys-from-a-personal-information-exchange-pfx-file-to-the-destination-store/>

Servidor

[crayon-6a9d57d9308d7218517148/]

Cliente

[crayon-6a9d57d9308de892894633/]

Windows PowerShell ISE

Archivo Editar Ver Herramientas Depurar Complementos Ayuda

Sin titulo1.ps1 X

```
1 ##Server
2 $port=2021
3 $endpoint = new-object System.Net.IPEndPoint ([IPAddress]::Any,$port)
4 $udpcClient=new-Object System.Net.Sockets.UdpClient $port
5
6 #Comprobar que el hash recibido y el hash del fichero recibido es correcto
7 $content=$udpcClient.Receive([ref]$endpoint)
8 $convert=[Text.Encoding]::ASCII.GetString($content)
9 $convert | Out-File ficheroRecibido.txt
10
11 #Para descifrar el mensaje es necesario tener el certificado
12 # https://www.jesusninoc.com/11/20/imports-certificates-and-private-keys-from-a-personal-information-exchange-pfx
13 Unprotect-CmsMessage -Path ficheroRecibido.txt
14
15 $udpcClient.Close()
```

```
PS C:\Users\juan> ##Server
$port=2021
$endpoint = new-object System.Net.IPEndPoint ([IPAddress]::Any,$port)
$udpcClient=new-Object System.Net.Sockets.UdpClient $port

#Comprobar que el hash recibido y el hash del fichero recibido es correcto
$content=$udpcClient.Receive([ref]$endpoint)
$convert=[Text.Encoding]::ASCII.GetString($content)
$convert | Out-File ficheroRecibido.txt

#Para descifrar el mensaje es necesario tener el certificado
# https://www.jesusninoc.com/11/20/imports-certificates-and-private-keys-from-a-personal-information-exchange-pfx
Unprotect-CmsMessage -Path ficheroRecibido.txt

$udpcClient.Close()
Hello

PS C:\Users\juan>
```

Completado Lin. 15 Col. 19 105 %

Windows PowerShell ISE

Archivo Editar Ver Herramientas Depurar Complementos Ayuda

Sin titulo1.ps1 X

```
1 ##Client
2 $port=2021
3 $endpoint = new-object System.Net.IPEndPoint ([IPAddress]::Loopback,$port)
4 $udpcClient=new-Object System.Net.Sockets.UdpClient
5
6 #Crear un certificado para firmar el mensaje
7 #https://www.jesusninoc.com/11/18/exports-a-certificate-to-a-personal-information-exchange-pfx
8 $cert = New-SelfSignedCertificate -DnsName jesusninoc2 -CertStoreLocation "Cert:\CurrentUser\My"
9
10 #Encrypts content by using the Cryptographic Message Syntax format
11 "Hello" | Protect-CmsMessage -To cn=jesusninoc2 -OutFile secret.txt
12
13 $val=[string](Get-Content secret.txt)
14
15 $b=[Text.Encoding]::ASCII.GetBytes($val.ToString())
16 $bytesSent=$udpcClient.Send($b,$b.Length,$endpoint)
17 $udpcClient.Close()
```

```
PS C:\Users\juan> ##Client
$port=2021
$endpoint = new-object System.Net.IPEndPoint ([IPAddress]::Loopback,$port)
$udpcClient=new-Object System.Net.Sockets.UdpClient

#Crear un certificado para firmar el mensaje
#https://www.jesusninoc.com/11/18/exports-a-certificate-to-a-personal-information-exchange-pfx
$cert = New-SelfSignedCertificate -DnsName jesusninoc2 -CertStoreLocation "Cert:\CurrentUser\My"

#Encrypts content by using the Cryptographic Message Syntax format
"Hello" | Protect-CmsMessage -To cn=jesusninoc2 -OutFile secret.txt

$val=[string](Get-Content secret.txt)

$b=[Text.Encoding]::ASCII.GetBytes($val.ToString())
$bytesSent=$udpcClient.Send($b,$b.Length,$endpoint)
$udpcClient.Close()

PS C:\Users\juan>
```

Lin. 17 Col. 19 95 %