```
Write-Host 'Configuring IIS with SSL/TLS Deployment Best Practices...'
Write-Host
'------------------------------------------------------------------------
-----------'

# Disable Multi-Protocol Unified Hello
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\Multi-Protocol Unified Hello\Server' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\Multi-Protocol Unified Hello\Server' -name Enabled -value 0 -
PropertyType 'DWord' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\Multi-Protocol Unified Hello\Server' -name 'DisabledByDefault' -value
1 -PropertyType 'DWord' -Force | Out-Null
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\Multi-Protocol Unified Hello\Client' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\Multi-Protocol Unified Hello\Client' -name Enabled -value 0 -
PropertyType 'DWord' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\Multi-Protocol Unified Hello\Client' -name 'DisabledByDefault' -value
1 -PropertyType 'DWord' -Force | Out-Null
Write-Host 'Multi-Protocol Unified Hello has been disabled.'

# Disable PCT 1.0
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\PCT 1.0\Server' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\PCT 1.0\Server' -name Enabled -value 0 -PropertyType 'DWord' -Force |
Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\PCT 1.0\Server' -name 'DisabledByDefault' -value 1 -PropertyType
'DWord' -Force | Out-Null
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\PCT 1.0\Client' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\PCT 1.0\Client' -name Enabled -value 0 -PropertyType 'DWord' -Force |
Out-Null
New-ItemProperty -path 'HKLM:
```

```
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\PCT 1.0\Client' -name 'DisabledByDefault' -value 1 -PropertyType
'DWord' -Force | Out-Null
Write-Host 'PCT 1.0 has been disabled.'

# Disable SSL 2.0 (PCI Compliance)
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 2.0\Server' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 2.0\Server' -name Enabled -value 0 -PropertyType 'DWord' -Force |
Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 2.0\Server' -name 'DisabledByDefault' -value 1 -PropertyType
'DWord' -Force | Out-Null
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 2.0\Client' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 2.0\Client' -name Enabled -value 0 -PropertyType 'DWord' -Force |
Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 2.0\Client' -name 'DisabledByDefault' -value 1 -PropertyType
'DWord' -Force | Out-Null
Write-Host 'SSL 2.0 has been disabled.'

# Disable SSL 3.0 (PCI Compliance) and enable "Poodle" protection
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 3.0\Server' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 3.0\Server' -name Enabled -value 0 -PropertyType 'DWord' -Force |
Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 3.0\Server' -name 'DisabledByDefault' -value 1 -PropertyType
'DWord' -Force | Out-Null
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 3.0\Client' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 3.0\Client' -name Enabled -value 0 -PropertyType 'DWord' -Force |
Out-Null
New-ItemProperty -path 'HKLM:
```

```
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\SSL 3.0\Client' -name 'DisabledByDefault' -value 1 -PropertyType
'DWord' -Force | Out-Null
Write-Host 'SSL 3.0 has been disabled.'

# Disable TLS 1.0 for client and server SCHANNEL communications
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Server' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Server' -name 'Enabled' -value '0' -PropertyType 'DWord' -
Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Server' -name 'DisabledByDefault' -value 1 -PropertyType
'DWord' -Force | Out-Null
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Client' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Client' -name 'Enabled' -value '0' -PropertyType 'DWord' -
Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Client' -name 'DisabledByDefault' -value 1 -PropertyType
'DWord' -Force | Out-Null
Write-Host 'TLS 1.0 has been disabled.'

# Add and Enable TLS 1.1 for client and server SCHANNEL communications
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Server' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Server' -name 'Enabled' -value '1' -PropertyType 'DWord' -
Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Server' -name 'DisabledByDefault' -value 0 -PropertyType
'DWord' -Force | Out-Null
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Client' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Client' -name 'Enabled' -value '1' -PropertyType 'DWord' -
Force | Out-Null
New-ItemProperty -path 'HKLM:
```

```
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Client' -name 'DisabledByDefault' -value 0 -PropertyType
'DWord' -Force | Out-Null
Write-Host 'TLS 1.1 has been enabled.'

# Add and Enable TLS 1.2 for client and server SCHANNEL communications
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Server' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Server' -name 'Enabled' -value '1' -PropertyType 'DWord' -
Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Server' -name 'DisabledByDefault' -value 0 -PropertyType
'DWord' -Force | Out-Null
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Client' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Client' -name 'Enabled' -value '1' -PropertyType 'DWord' -
Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Client' -name 'DisabledByDefault' -value 0 -PropertyType
'DWord' -Force | Out-Null
Write-Host 'TLS 1.2 has been enabled.'


# Re-create the ciphers key.
New-Item
'HKLM:SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciph
ers' -Force | Out-Null

# Disable insecure/weak ciphers.
$insecureCiphers = @(
  'DES 56/56',
  'NULL',
  'RC2 128/128',
  'RC2 40/128',
  'RC2 56/128',
  'RC4 40/128',
  'RC4 56/128',
  'RC4 64/128',
  'RC4 128/128'
)
Foreach ($insecureCipher in $insecureCiphers) {
  $key = (Get-Item HKLM:
```

```
\).OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Ciphers', $true).CreateSubKey($insecureCipher)
  $key.SetValue('Enabled', 0, 'DWord')
  $key.close()
  Write-Host "Weak cipher $insecureCipher has been disabled."
}

# Enable new secure ciphers.
# - RC4: It is recommended to disable RC4, but you may lock out WinXP/
IE8 if you enforce this. This is a requirement for FIPS 140-2.
# - 3DES: It is recommended to disable these in near future. This is
the last cipher supported by Windows XP.
# - Windows Vista and before 'Triple DES 168' was named 'Triple DES
168/168' per https://support.microsoft.com/en-us/kb/245030
$secureCiphers = @(
  'AES 128/128',
  'AES 256/256',
  'Triple DES 168'
)
Foreach ($secureCipher in $secureCiphers) {
  $key = (Get-Item HKLM:
\).OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Ciphers', $true).CreateSubKey($secureCipher)
  New-ItemProperty -path "HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\
$secureCipher" -name 'Enabled' -value '0xffffffff' -PropertyType
'DWord' -Force | Out-Null
  $key.close()
  Write-Host "Strong cipher $secureCipher has been enabled."
}

# Set hashes configuration.
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes' -
Force | Out-Null
New-Item 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD
5' -Force | Out-Null
New-ItemProperty -path 'HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD
5' -name Enabled -value 0 -PropertyType 'DWord' -Force | Out-Null

$secureHashes = @(
  'SHA',
  'SHA256',
  'SHA384',
  'SHA512'
)
Foreach ($secureHash in $secureHashes) {
  $key = (Get-Item HKLM:
```

```
\).OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Hashes', $true).CreateSubKey($secureHash)
  New-ItemProperty -path "HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\
$secureHash" -name 'Enabled' -value '0xffffffff' -PropertyType 'DWord'
-Force | Out-Null
  $key.close()
  Write-Host "Hash $secureHash has been enabled."
}

# Set KeyExchangeAlgorithms configuration.
New-Item
'HKLM:SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyE
xchangeAlgorithms' -Force | Out-Null
$secureKeyExchangeAlgorithms = @(
  'Diffie-Hellman',
  'ECDH',
  'PKCS'
)
Foreach ($secureKeyExchangeAlgorithm in $secureKeyExchangeAlgorithms)
{
  $key = (Get-Item HKLM:
\).OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\KeyExchangeAlgorithms',
$true).CreateSubKey($secureKeyExchangeAlgorithm)
  New-ItemProperty -path "HKLM:
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchan
geAlgorithms\$secureKeyExchangeAlgorithm" -name 'Enabled' -value
'0xffffffff' -PropertyType 'DWord' -Force | Out-Null
  $key.close()
  Write-Host "KeyExchangeAlgorithm $secureKeyExchangeAlgorithm has
been enabled."
}

# Set cipher suites order as secure as possible (Enables Perfect
Forward Secrecy).

  Write-Host 'Use cipher suites order for Windows
2008/2008R2/2012/2012R2.'
  $cipherSuitesOrder = @(
  'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521',
    'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384',
    'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521',
    'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384',
    'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256',
    'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521',
    'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384',
    'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256',
    'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521',
    'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384',
```

```
    'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256',
    'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521',
    'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384',
    'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256',
    'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521',
    'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384',
    'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256',
    'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521',
    'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384',
    'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521',
    'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384',
    'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256',
    'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521',
    'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384',
    'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256',
    'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521',
    'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384',
    'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256',
    'TLS_RSA_WITH_AES_256_GCM_SHA384',
    'TLS_RSA_WITH_AES_128_GCM_SHA256',
    'TLS_RSA_WITH_AES_256_CBC_SHA256',
    'TLS_RSA_WITH_AES_128_CBC_SHA256',
    'TLS_RSA_WITH_AES_256_CBC_SHA',
    'TLS_RSA_WITH_AES_128_CBC_SHA'

  )
$cipherSuitesAsString = [string]::join(',', $cipherSuitesOrder)
# One user reported this key does not exists on Windows 2012R2. Cannot
repro myself on a brand new Windows 2012R2 core machine. Adding this
just to be save.
New-Item 'HKLM:
\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002'
-ErrorAction SilentlyContinue
New-ItemProperty -path 'HKLM:
\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002'
-name 'Functions' -value $cipherSuitesAsString -PropertyType 'String'
-Force | Out-Null

Write-Host -ForegroundColor Red 'A computer restart is required to
apply settings. Restart computer now?'
Restart-Computer -Force -Confirm
```