IIS’de HTTPS Yapma, Güvensiz SSL/TLS Protokolleri Deaktif Yapma ve SSL/TLS Protokollerindeki Güvensiz Şifrelemeleri Deaktif Yapma

(+) Bu uygulama birebir denenmiştir ve başarıyla uygulanmıştır.

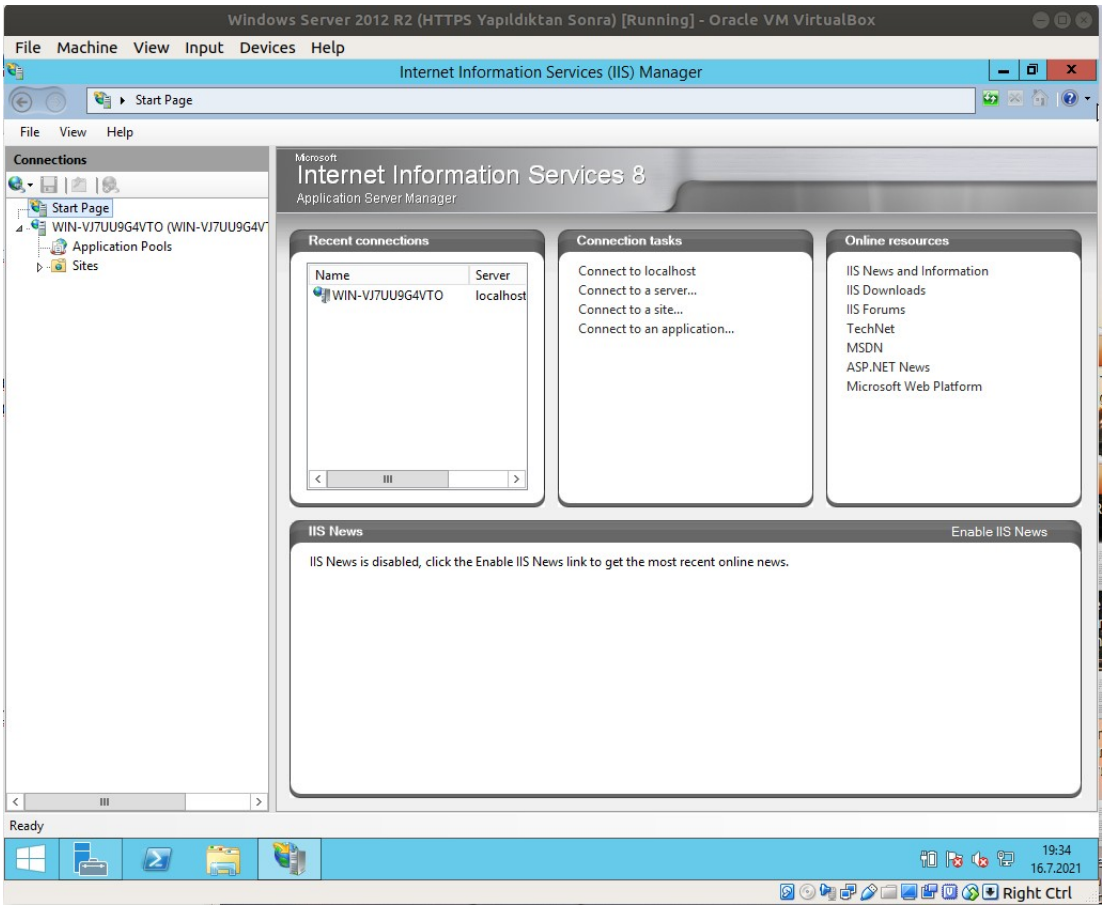
Gereksinimler

Ubuntu 18.04 LTS - Nmap SSL-ENUM-CIPHER Script’i (Ana Makine)
Windows Server 2012 R2 VM (Sanal Makinesi) // Örnek Windows IIS Makine

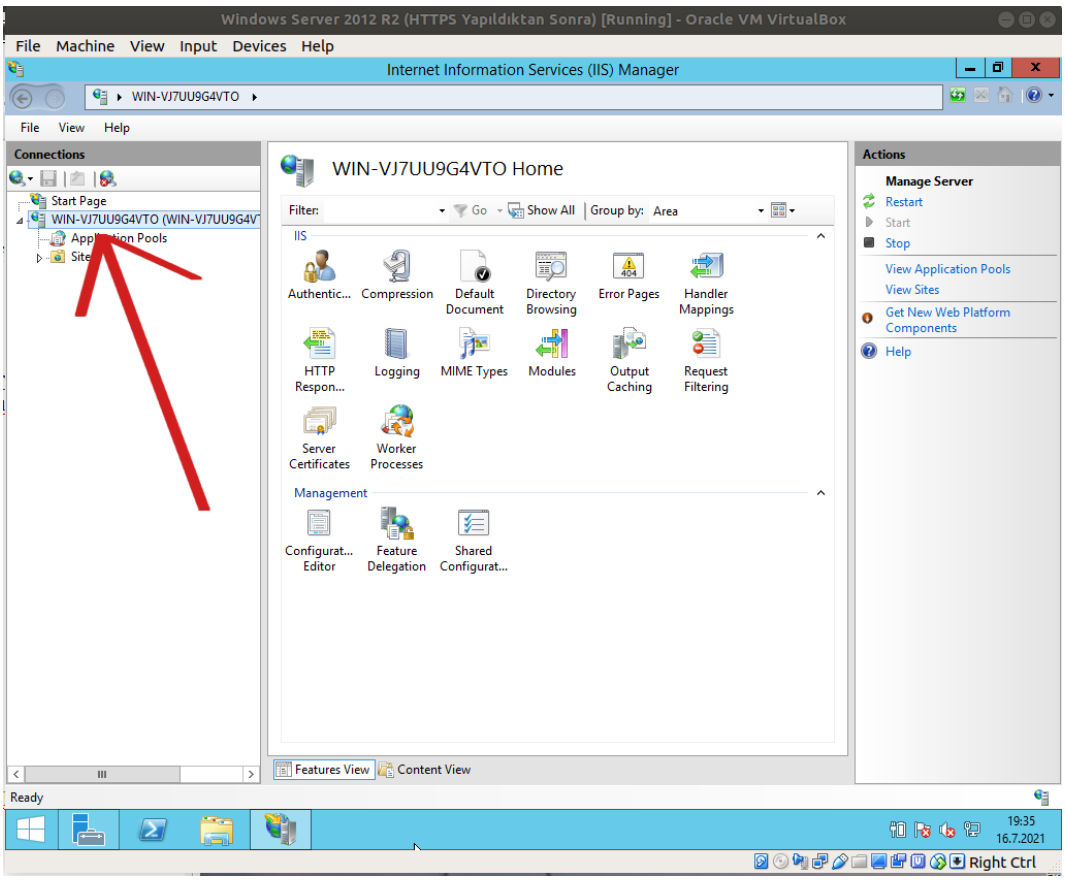
a. IIS’de HTTPS Açma

Windows Server makinelerde IIS Yöneticisi’nden hizmet olarak sunulan web siteye erişimin https üzerinden olabilmesi özelliği açılabilir. Bu işlemler IIS Yöneticisi’nden uygulanır. Adımlar şu şekildedir:

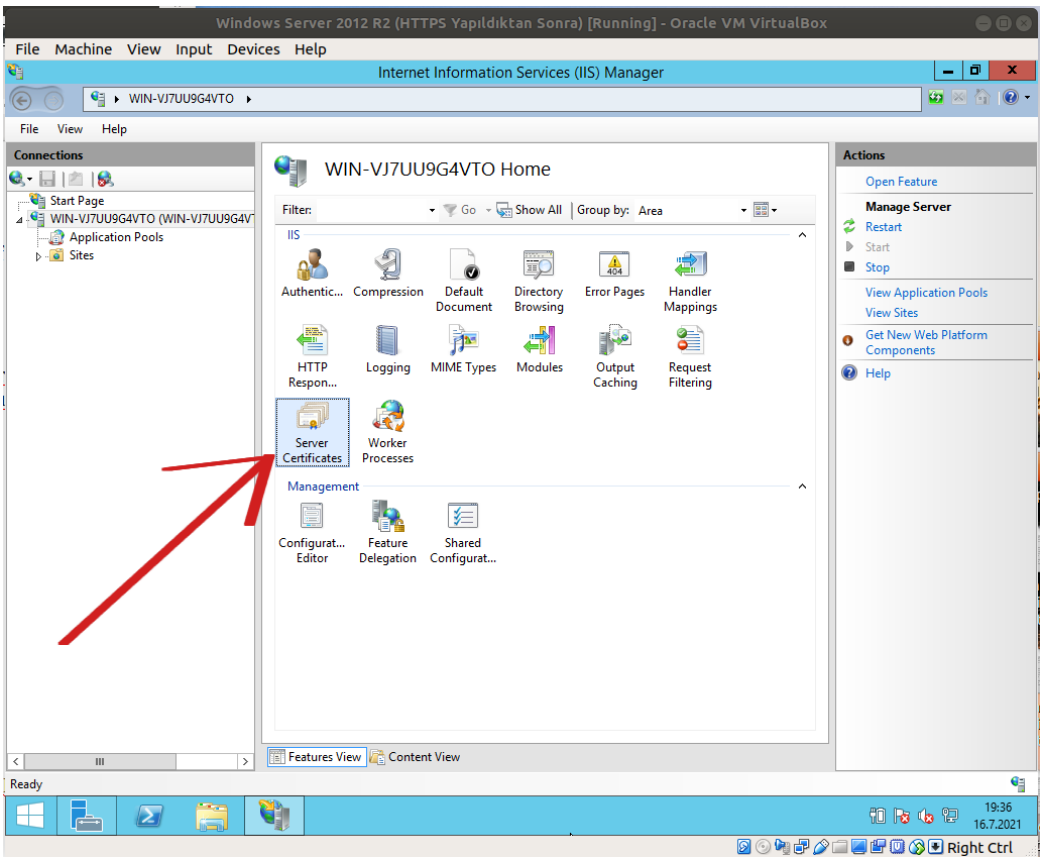
- IIS Manager açılır.



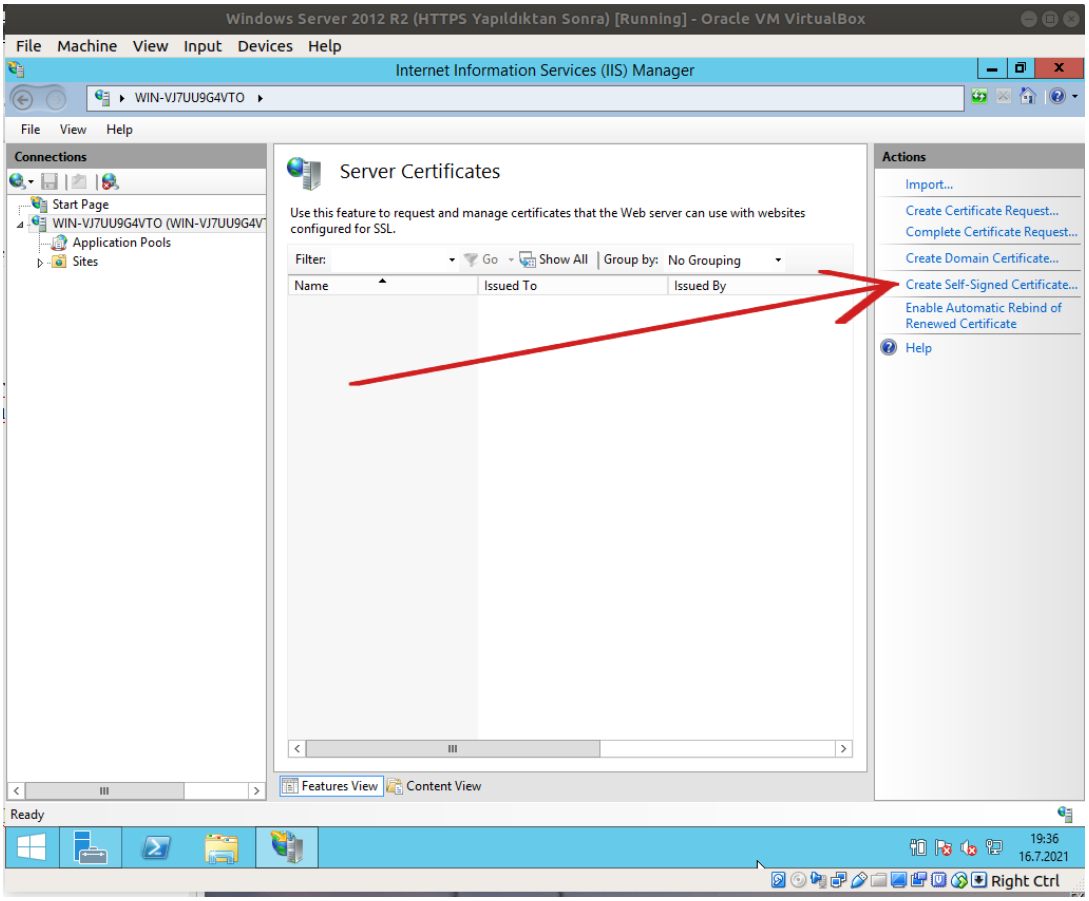
- Sol sütunda “server” seçilir.



- Açılan ekranda "Server Certificates"e girilir.

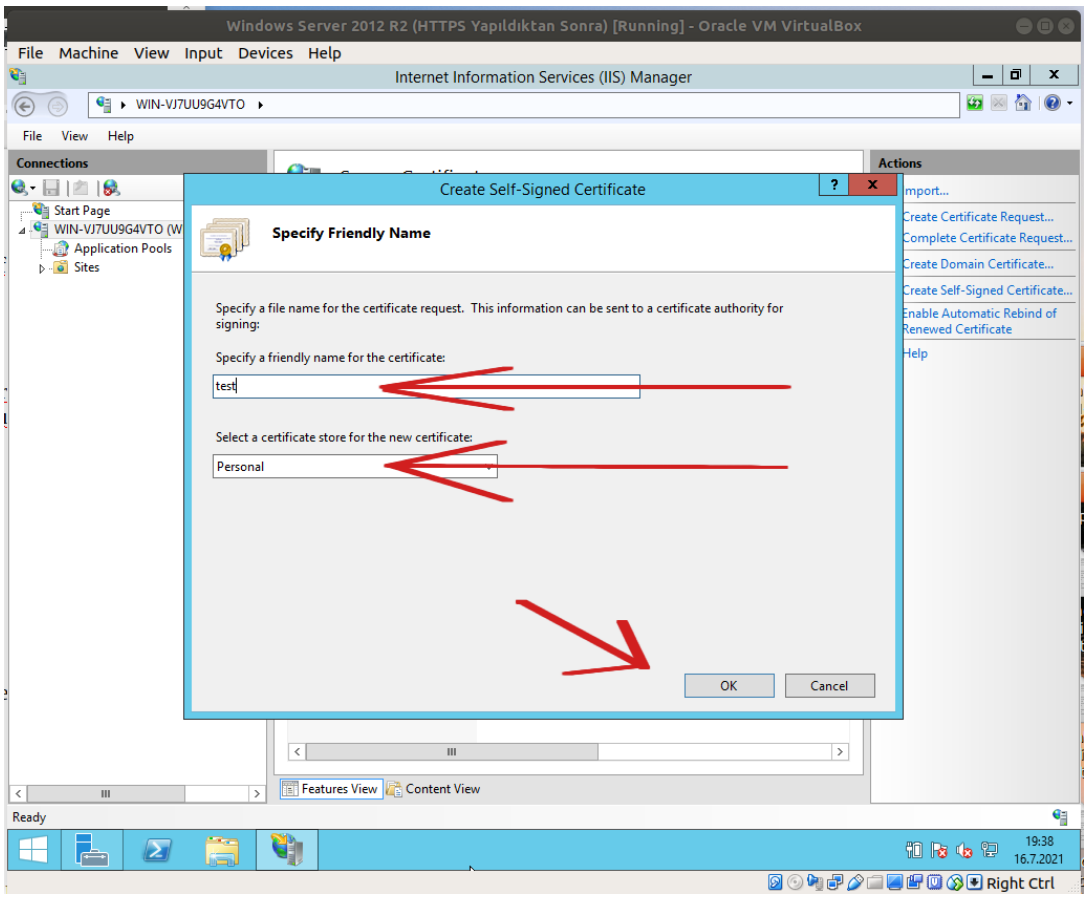


- Sağ sütundaki "Create a self signed certificate" seçilir.

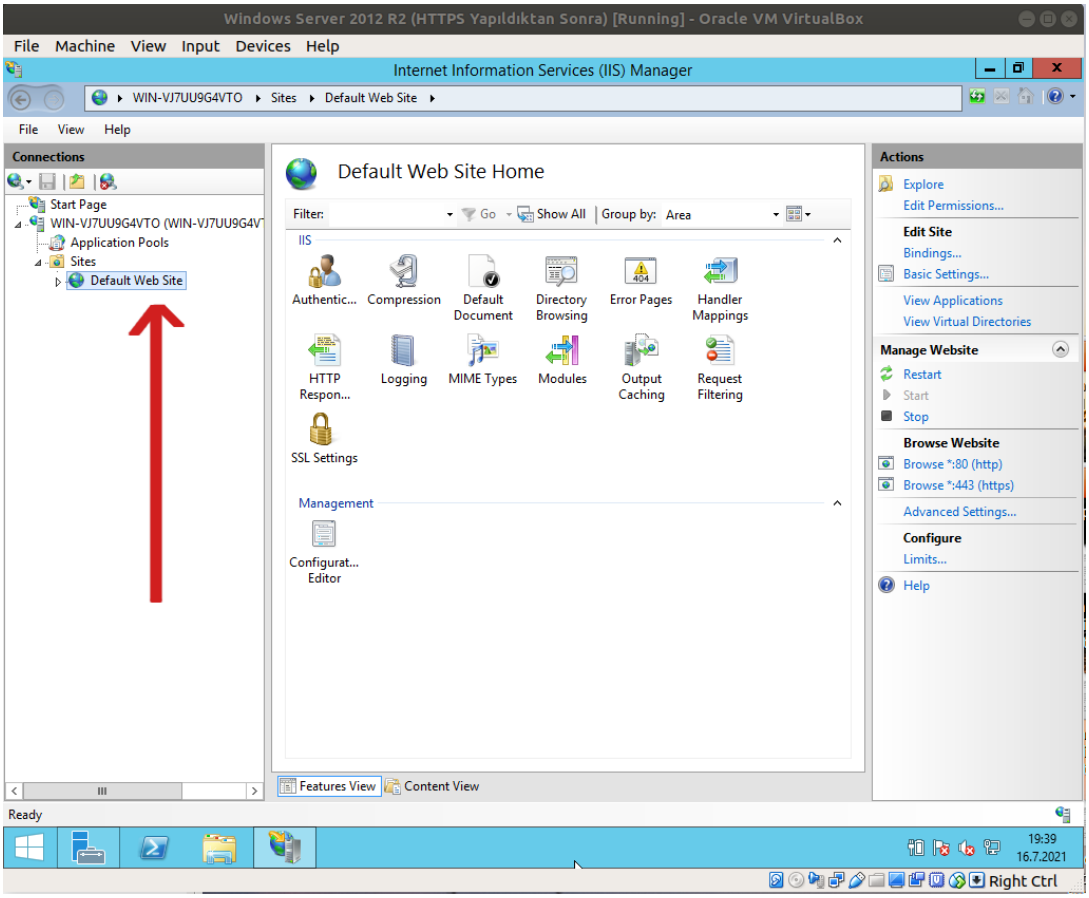


Not: Test web sunucusu olduğundan self signed sertifika oluşturulur. Internete açık web sunucu için Create Certificate Request üzerinden adımlar ilerler.

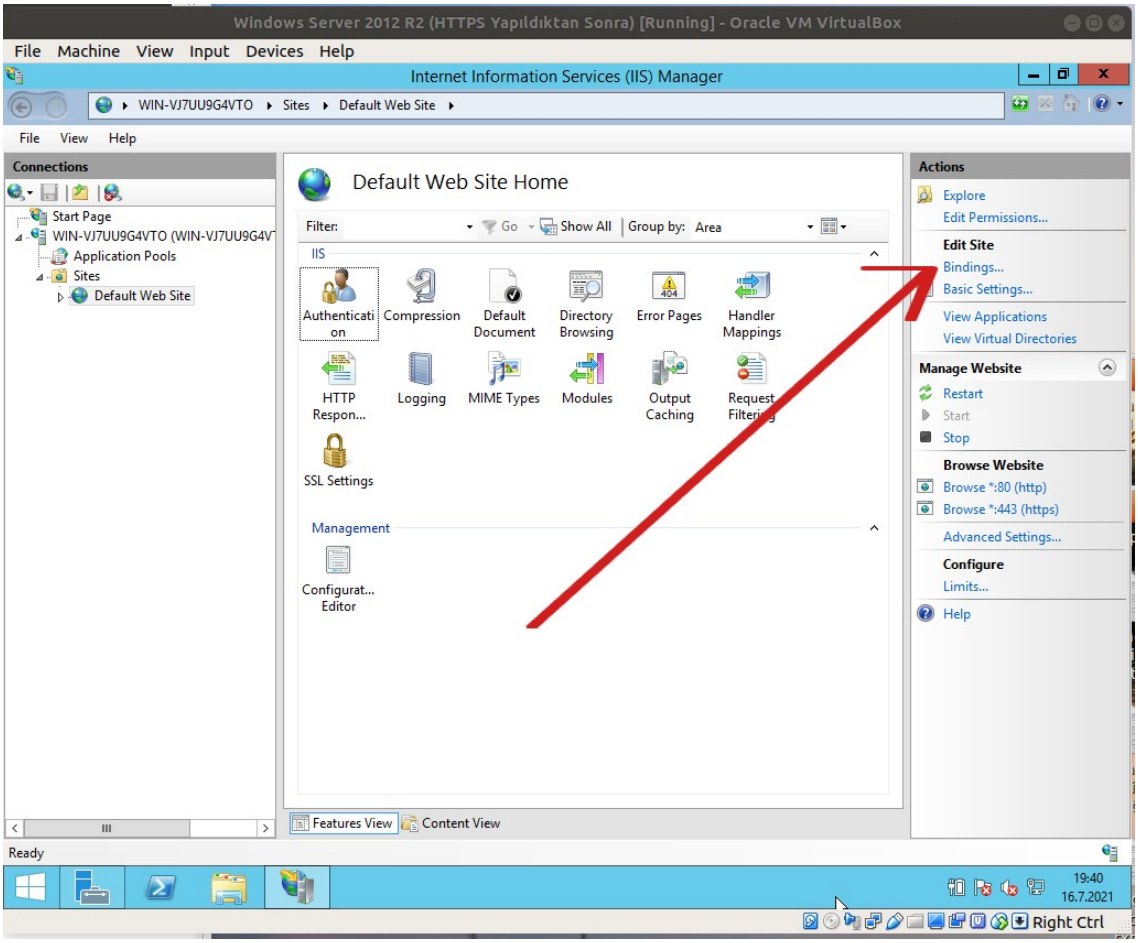
- Self signed sertifika için isim girilir ve sertifikanın depolanacağı yer olarak Personel denilir.



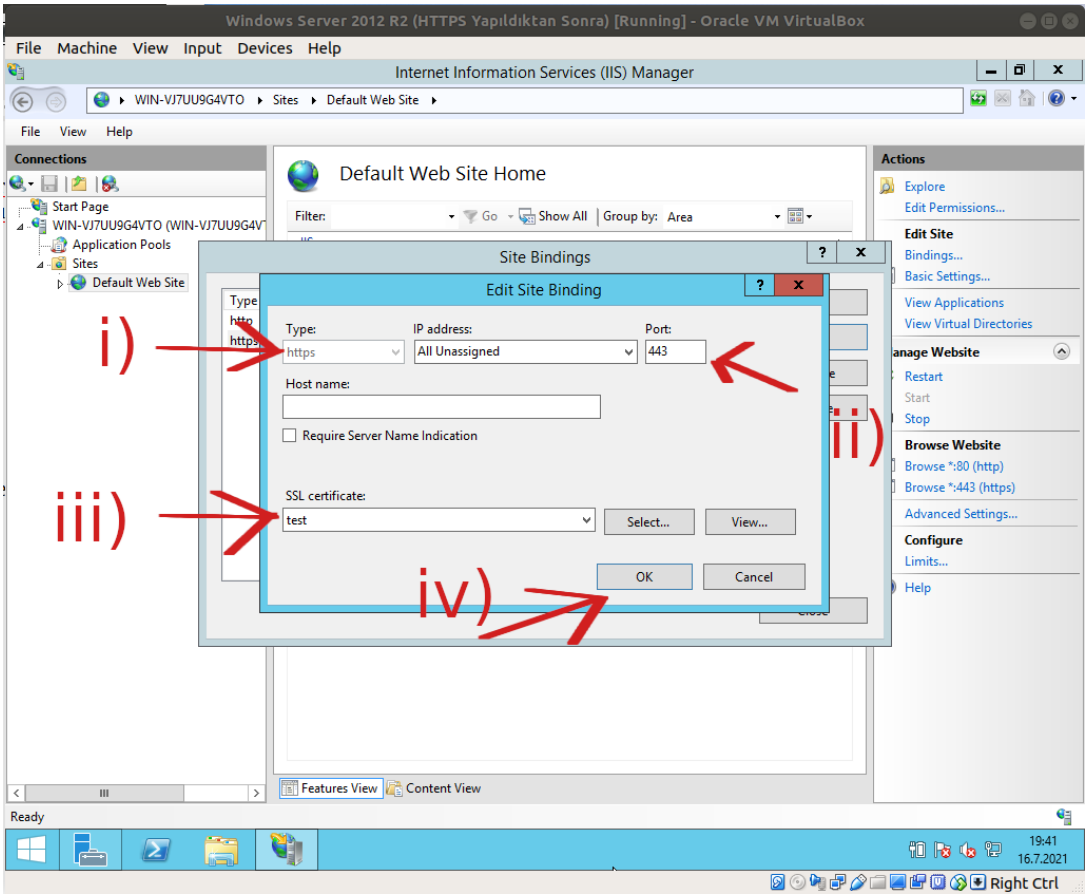
- Sol sütundan Sites->Default Web Site'a gidilir.



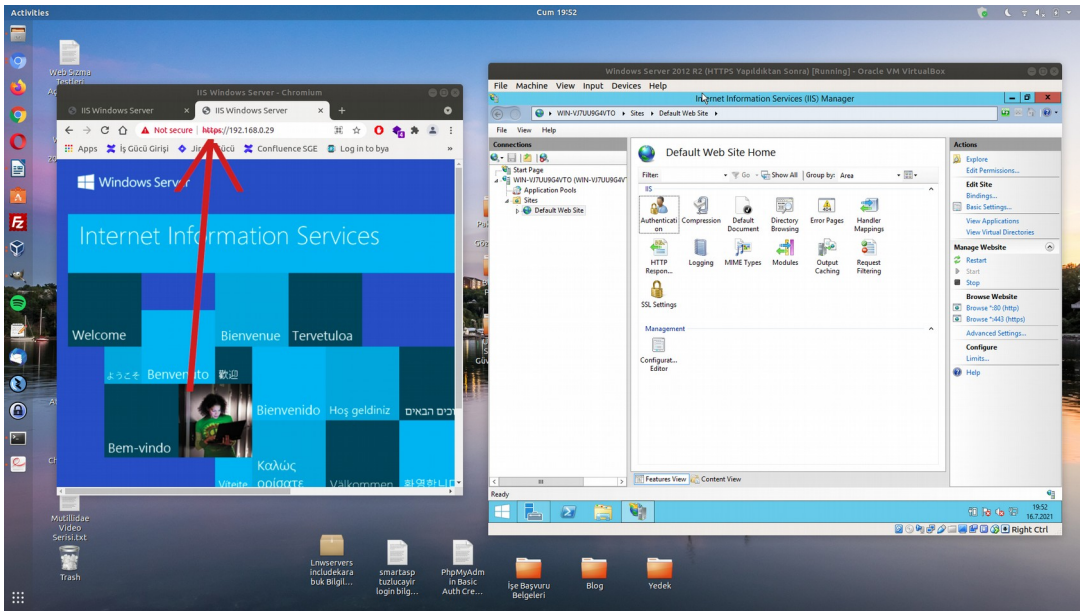
- Açılan ekranda sağ sütundaki “Bindings”e tıklanır.



- Add denilir. Https port 443, ve oluşturulan self signed sertifikası seçimi yapılır.



Bu işlemler sonrası windows server makinenin web hizmetine https üzerinden gidilebilirdir.



b. Güvensiz SSL/TLS Protokolleri Deaktif Yapma

Öncelikle https olan windows server 2012 R2 web sunucuda aktif olan tüm ssl/tls protokollerini görelim.

Ubuntu 18.04 LTS Ana Makine:

> nmap --script ssl-enum-ciphers -p 443 192.168.0.29 // Windows Server 2012 R2 IP'si

Çıktı:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-07-16 17:13 +03
Nmap scan report for 192.168.0.29
Host is up (0.00034s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
```

```
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|     TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|   compressors:
|     NULL
|   cipher preference: server
|   warnings:
|     64-bit block cipher 3DES vulnerable to SWEET32 attack
|     Broken cipher RC4 is deprecated by RFC 7465
|     Ciphersuite uses MD5 for message integrity
|     Weak certificate signature: SHA1
|_  least strength: C
MAC Address: 08:00:27:D4:54:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
```

Bu kullanılan protokollerden güvensiz olanları web sunucuda kapatalım. Adımlar şu şekildedir:

- SSLv3'ü deaktif etmek için;

    i) Çalıştır->Regedit açılır ve,

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\

    dizinine gidilir. SSL 3.0 klasörü yoksa New->Key ile oluşturulur.

    ii) SSL 3.0 içerisinde Server klasörü yoksa New->Key ile oluşturulur.

    iii) Server klasörü içerisinde Enabled dosyası yoksa New->DWORD ile oluşturulur ve değeri 0 yapılır.

- TLSv1.0'ı deaktif etmek için;

    i) Çalıştır->Regedit açılır ve,

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\

    dizinine gidilir. TLS 1.0 klasörü yoksa New->Key ile oluşturulur.

    ii) TLS 1.0 içerisinde Server klasörü yoksa New->Key ile oluşturulur.

    iii) Server klasörü içerisinde Enabled dosyası yoksa New->DWORD ile oluşturulur ve değeri 0 yapılır.

- TLSv1.1'i deaktif etmek için;

    i) Çalıştır->Regedit açılır ve,

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\

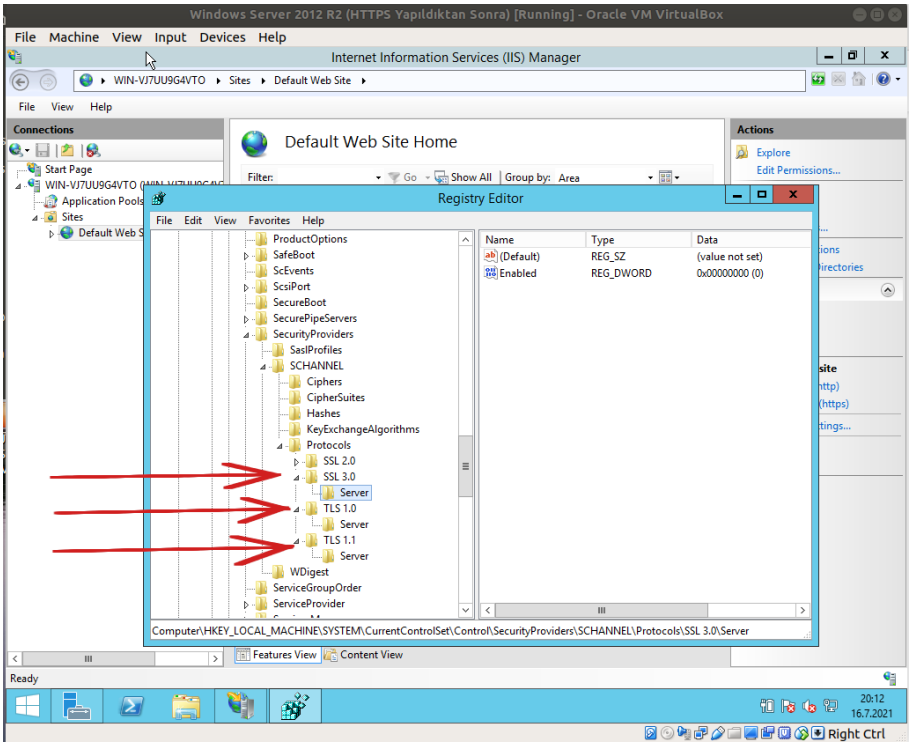
    dizinine gidilir. TLS 1.1 klasörü yoksa New->Key ile oluşturulur.

    ii) TLS 1.1 içerisinde Server klasörü yoksa New->Key ile oluşturulur.

iii) Server klasörü içerisinde Enabled dosyası yoksa New->DWORD ile oluşturulur ve değeri 0 yapılır.

Son olarak değişikliklerin etkinleşmesi için sistemin restart'lanması gerekir.

Nihai hal aşağıdaki gibi olacaktır. Her Server klasörünün içerisinde Enabled dosyası değeri 0 şeklinde olur.



Sistem restart'laması sonrası değişikliklerin geçerli olup olmadığını görmek için windows server makinesindeki aktif ssl/tls protokollerini tekrar denetleyelim.

Ubuntu 18.04 LTS Ana Makine:

> nmap --script ssl-enum-ciphers -p 443 192.168.0.29 // Windows Server 2012 R2 IP'si

Çıktı:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-07-16 17:27 +03
Nmap scan report for 192.168.0.29
Host is up (0.00035s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
```

```
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|_  least strength: C
MAC Address: 08:00:27:D4:54:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds
```

Görüldüğü gibi aktif ssl/tls protokolleri sadece güvenli olan TLSv1.2 şeklinde olmuştur.

Ek:

Kayıt defterinde hatalı değişiklik yapmak dikkatli olunmazsa sisteme kalıcı hasar verebilir. Bu nedenle yedekli çalışmalıdır. Kayıt defterinde değişiklik yapılacak ilgili kök klasörün yedeği alınmalıdır ve sonra değişiklikler o ilgili kök klasörde uygulanmalıdır. Herhangi bir hatalı değiştirme sonucu hasar söz konusu olduğunda yedek dosya geri yüklenerek kayıt defterindeki ilgili kök klasör eski halini alacaktır ve sorun çözümlenecektir. Bunun için;

i) Çalıştır->Regedit açılır ve,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\

dizinine sağ tık yapılır.

ii) Export seçeneği seçilir ve yedekleme dosyasının konumu, sonra adı belirlenir.

iii) Ardından uygulanan değişiklikler bir soruna yol açarsa değişiklikleri geri almak için Regedit->File->Import ile yedek dosya seçilir ve yüklenir.

Böylece eski değerler kayıt defterine yazılacaktır ve soruna yol açan değişiklik geri alınmış olacaktır.

Benim Not:

(*) Birebir denenmiştir ve başarıyla uygulanmıştır.

Denemek maksatlı Protocols altındaki SSL 3.0, TLS 1.0 ve TLS 1.1 regedit yedeği Protocols'a sağ tık yapıp Export ile alınmıştır ve ardından regedit'te Protocols altındaki Enabled dosyalarına 0 yerine değiştirmek maksatlı 1 değerleri girilmiştir. Ardından Regedit->File->Import ile yedek dosya yüklendiğinde Protocols altındaki Enabled dosya değerleri hepsi tekrar eski haline 0'a dönmüştür. Yani uygulanan değişiklikler yedek dosya ile geri alınabilmiştir.

c. SSL/TLS Protokollerindeki Güvensiz Şifrelemeleri Deaktif Yapma

Güvensiz ssl/tls protokolleri deaktif edildikten sonra geriye kalan güvenli tls protokolü TLSv1.2 için bu protokolde kullanılan güvensiz şifreleme algoritmaları da deaktif edilmelidir. Böylece tam güvenli bir ssl/tls sertifikasyon yapılandırılmasına gidilmiş olacaktır. Bu işlem için https olan windows server 2012 R2 web sunucuda aktif olan tüm ssl/tls protokollerini tekrar görelim.

Ubuntu 18.04 LTS Ana Makine:

> nmap --script ssl-enum-ciphers -p 443 192.168.0.29 // Windows Server 2012 R2 IP'si

Çıktı:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-07-17 14:50 +03
Nmap scan report for 192.168.0.30
Host is up (0.00030s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|_  least strength: C
MAC Address: 08:00:27:D4:54:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

Olması gerektiği gibi sadece tls 1.2 aktiftir, fakat tls 1.2 protokolünün kullandığı şifrelemelerde C notuna sahip olanlar vardır. Bunların sadece A olması gerekmektedir. Bunun için kayıt defterinden aynı yöntemle yine ayarlar yapılmaktadır ve web sunucu sistemi komple yeniden başlatılarak işlem etkinleştirilmektedir. Adımlar şu şekildedir:

i) Çalıştır->Regedit açılır ve,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\

dizinine gidilir. Ardından New->Key ile şu isimde klasörler oluşturulur.

NULL
DES 56/56
RC2 40/128
RC2 56/128

RC2 128/128
RC4 40/128
RC4 56/128
RC4 64/128
RC4 128/128
Triple DES 168

ii) Ardından

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\

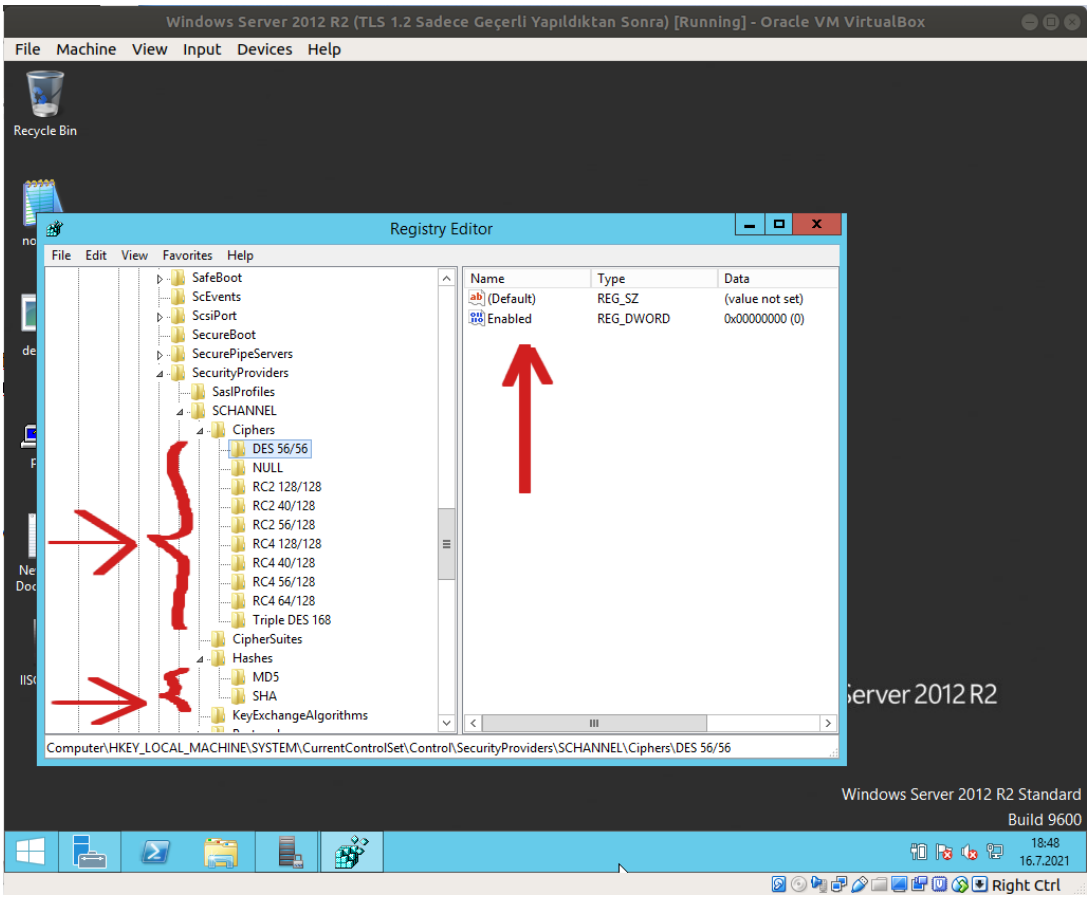
dizinine gidilir ve New->Key ile şu isimde klasörler oluşturulur.

MD5
SHA

ii) Son olarak tüm bu Ciphers\ ve Hashes\'da oluşturulan klasörlerin içerisinde New->DWORD ile Enabled isimli dosya oluşturulur ve değerleri 0 bırakılır.

Son olarak değişikliklerin etkinleşmesi için sistemin restart'lanması gerekir.

Nihai hal aşağıdaki gibi olur. Her şifreleme ve özet alma klasörünün içerisinde Enabled dosyası değeri 0 şeklinde olur.



Sistem restart'laması sonrası değişikliklerin geçerli olup olmadığını görmek için windows server makinesindeki aktif ssl/tls protokollerini tekrar denetleyelim.

Ubuntu 18.04 LTS Ana Makine:

> nmap --script ssl-enum-ciphers -p 443 192.168.0.29 // Windows Server 2012 R2 IP'si

Çıktı:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-07-17 14:59 +03
Nmap scan report for 192.168.0.30
Host is up (0.00033s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       Weak certificate signature: SHA1
|_  least strength: A
MAC Address: 08:00:27:D4:54:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
```

Görüldüğü gibi aktif ssl/tls protokolleri sadece güvenli olan TLSv1.2 şeklinde ve TLSv1.2'nin kullandığı şifreleme algoritmaları not seviyesi A şeklinde. Güvensiz C notlu zayıf şifreleme algoritmaları düzenleme sonrası deaktif duruma gelmiştir. Bu şekilde tam güvenli bir ssl/tls sertifikasyonu yapılandırması uygulanabilir.

Bir Tecrübe:

Zayıf şifreleme algoritmaları varken ve sonra yokken Netsparker taraması sonrası raporlamasıyla doğrulamak için Windows Server 2012 R2 sanal makinesindeki web hizmetini netsparker VM ile taradığımda web hizmetinde güçlü şifreleme algoritmalarıyla beraber zayıf şifreleme algoritmaları varken "Weak Ciphers Enabled" açıklığı bulgulandığı gibi sadece güçlü şifreleme algoritmaları varken yine "Weak Ciphers Enabled" demekte. Manual olarak Local Group Policy'den (gpedit.msc'den) Computer Configuration->Administrative Templates->Network->SSL Cipher Suite Order'a gidildiğinde manuel olarak şifreleme takımları isimleriyle belirtildiğinde dahi hep eklenen tüm şifreleme algoritmaları için "Weak Ciphers Enabled" demekte ve açıklığın bulgusu olarak şifreleme takımı olarak ne konulmuşsa tümünü her defasında zayıf şifreleme diye listelemekte.

> Not: Local Group Policy'den şifreleme algoritmalarının öncelik sırası ayarlanmakta. Aynı şekilde hangi şifreleme algoritması kullanılsın bilgisi de verilmiş olmakta.

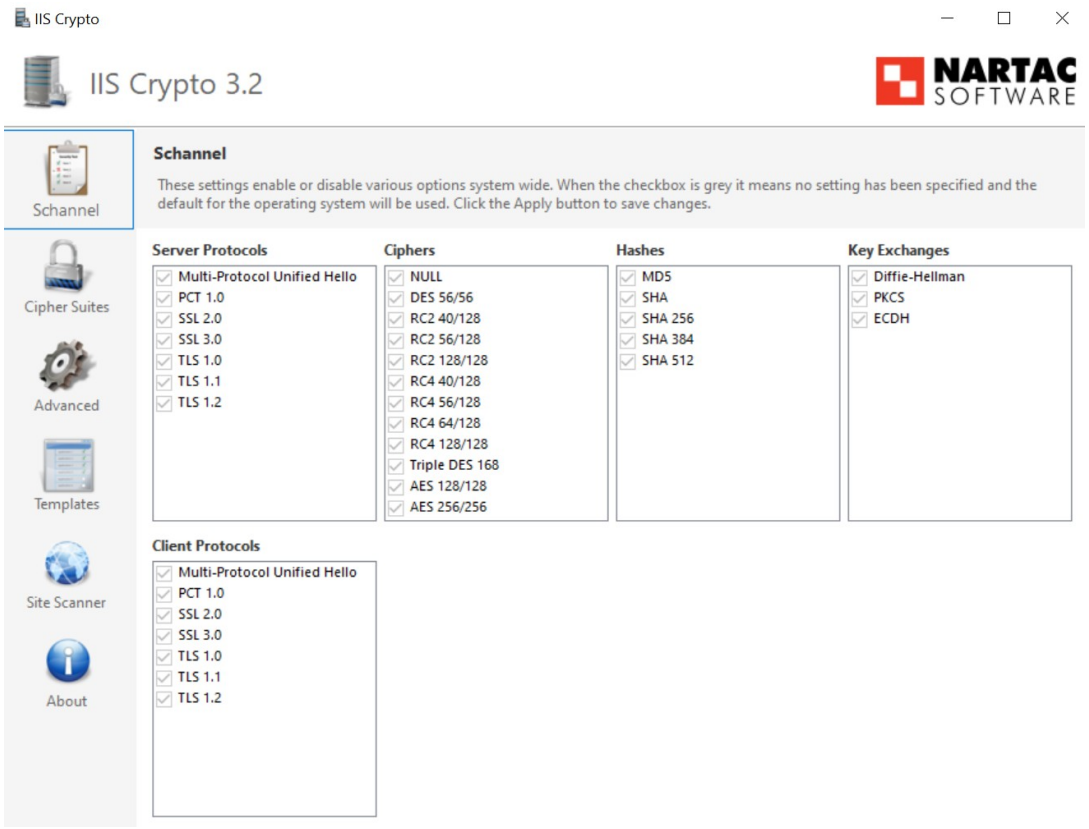
Yani web hizmeti hangi şifreleme algoritmasını kullanıyor olursa olsun hep kullandığı tüm şifreleme algoritmaları için zayıf şifreleme diyor ve Weak Ciphers Enabled altında paylaşıyor. Bu nedenle zayıf şifreleme açıklığı denetiminde Nmap ssl-enum-ciphers referans alınabilir.

Ekstra

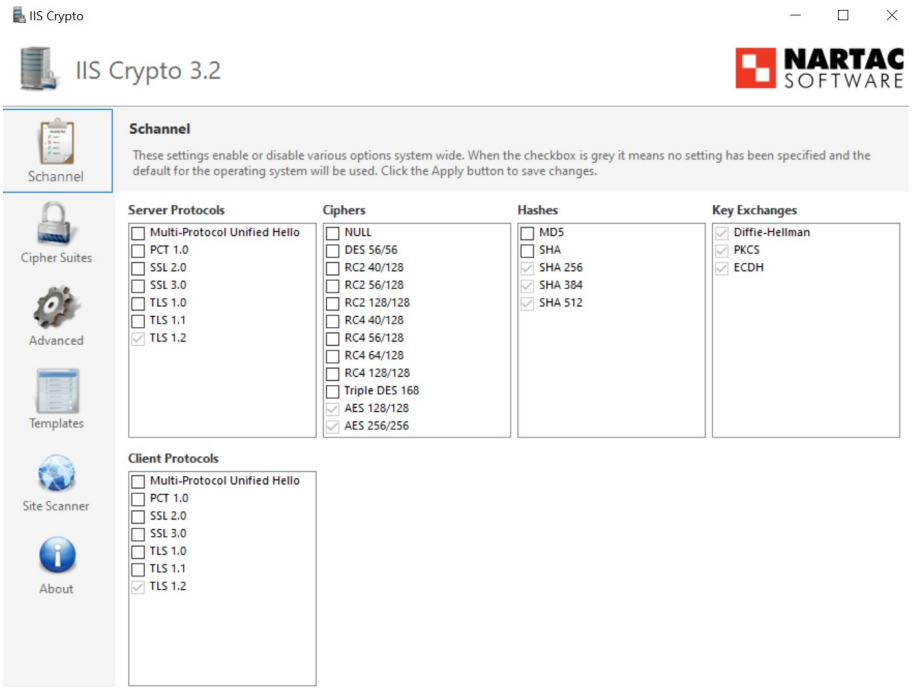
Güvenli ssl/tls protokolünü ve sonra güvenli şifreleme algoritmalarını aktif bırakıp, geri kalanı deaktif etmek için kayıt defterinden ayarlamalar yapıldı. Bu işlemin aynısı IIS Crypto adındaki bir uygulama ile görsel arayüzden de yapılabilir.

İndirme Linki:

https://www.nartac.com/Products/IISCrypto/Download



IIS Crypto uygulaması kayıt defterinde bizim yaptığımız güncellemeleri yapar. Dikkat edilirse sol tarafta Schannel menüsü vardır. Bu kayıt defterinde düzenleme yaparken kullandığımız klasördür. Arayüzdeki protokoller ve şifreleme algoritmalarından güvensiz olanlarda tick aşağıdaki gibi kaldırılarak elle yapılan güvensiz protokol ve güvensiz şifreleme algoritması deaktif işleminin aynısı görsel olarak uygulanabilir. Yazılım arkaplanda elle kayıt defterinde yaptığımız düzenlemeleri yapacaktır.



Yukarıdaki güvenli ayarlama yapılmadan önce Windows Server 2012 R2 VM'de snapshot'a dönülmüştür ve tls v1.2 aktifken, fakat zayıf şifreleme algoritmaları mevcutken nmap ssl-enum-ciphers denetlemesi yapılmıştır. Ardından ayarlamalar yapılıp reboot yapıldığında nmap ssl-enum-ciphers denetlemesi tekrar yapılmıştır ve güvensiz yapılandırma çıktısı sonrası güvenli yapılandırma çıktısı alınabilmiştir.

Ubuntu 18.04 LTS Ana Makine:

> nmap --script ssl-enum-ciphers -p 443 192.168.0.29 // Windows Server 2012 R2 IP'si

Çıktı:

Starting Nmap 7.60 (https://nmap.org) at 2021-07-17 14:59 +03
Nmap scan report for 192.168.0.30
Host is up (0.00033s latency).

PORT STATE SERVICE
443/tcp open https
| ssl-enum-ciphers:
| TLSv1.2:
| **ciphers:**
| **TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A**
| **TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A**
| **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A**
| compressors:
| NULL
| cipher preference: server
| warnings:
| Weak certificate signature: SHA1
|_ **least strength: A**
MAC Address: 08:00:27:D4:54:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds

Kaynaklar

https://us.informatiweb-pro.net/system-admin/win-server/ws-2012-secure-your-web-server-with-ssl-https.html

https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-sslv3/

https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-10/

https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-11/

https://support.microsoft.com/en-us/topic/how-to-back-up-and-restore-the-registry-in-windows-855140ad-e318-2a13-2829-d428a2ab0692#:~:text=Back%20up%20the%20registry%20manually,-From%20the%20Start&text=In%20Registry%20Editor%2C%20locate%20and,Click%20Save.

https://www.linkedin.com/pulse/remediation-ssltls-related-vulnerabilities-using-iis-crypto-siva

https://www.howtogeek.com/221080/how-to-update-your-windows-server-cipher-suite-for-better-security/

https://www.youtube.com/watch?v=zB4fYkfWcAw&ab_channel=RobertMcMillen