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.

Windov	vs Server 2012 R2 (HTTPS Yapıldıktan Sonra) [Running] - Oracle VM VirtualBox	
File Machine View Input Device	es Help	
	Internet Information Services (IIS) Manager	
WIN-VJ7UU9G4VTO ►		🖅 🖄 🔞 🕐 🔻
File View Help		
Connections	WIN-VJ7UU9G4VTO Home Filter: • • •	Actions Manage Server Restart Start Stop View Application Pools View Sites Get New Web Platform Components Help
Ready		6 ₁
		19:35 🕞 😼 19:35 16.7.2021
	🖸 🕑 🖣 🗗 🏈 I	💷 🛃 🖽 🔟 🐼 💽 Right Ctrl

- Açılan ekranda "Server Certificates"e girilir.

Windo		× 080
File Machine View Input Devi	ces Help	
	Internet Information Services (IIS) Manager	_ 0 ×
WIN-VJ7UU9G4VTO ►		🗾 🖸 🖄 🔞 🔹
File View Help		
Connections		Actions
		Open Feature
Start Page	Filter: • 🐨 Go - 🥁 Show All Group by: Area - 📰 -	Manage Server
Application Pools	115	Restart Start
⊳ - 🙋 Sites	🔏 🦪 🔒 🕎 🔝 🚚	Stop
	Authentic Compression Default Directory Error Pages Handler	View Application Pools
	Document Browsing Mappings	View Sites
	🕋 🎚 🏂 📫 🌮 籠	Get New Web Platform Components
	HTTP Logging MIME Types Modules Output Request Respon Caching Filtering	🕡 Help
<u>.</u>		
	Certificates Processes	
	Management	
	Configurat Feature Shared	
	Editor Delegation Configurat	
	Features View 💦 Content View	
Ready		¢:
	V)	19:36 16.7.2021
		🔉 🖃 🖳 🕼 🔇 🖲 Right Ctrl

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

Window	ws Server 2012 R2 (HTTPS Yapıldıktan Sonra) [Running] - Oracle VM VirtualBox	•••
File Machine View Input Devic	es Help	
v	Internet Information Services (IIS) Manager	
WIN-VJ7UU9G4VTO ►		🐱 🖄 🚯 🕶
File View Help		
Connections	Server Certificates	ctions Import
Start Page Start Page WIN-VJ7UU9G4VTO (WIN-VJ7UU9G4V Application Pools	Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.	Create Certificate Request Complete Certificate Request
b - i Sites	Filter:	Create Domain Certificate
	Name A Issued To Issued By	Create Self-Signed Certificate
		Enable Automatic Rebind of Renewed Certificate
< <u>III</u> >	< III > Features View Content View	
Ready		9 <u>1</u>
	N	19:36 🔁 19:36 16.7.2021
		🚄 📴 🕼 🗣 Right Ctrl 👘

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.

File Machine View Input Devices Help			
Internet Information Services (IIS) Manager Image: Control of the services (IIS) Manager <th>File Machine View</th> <th>Input Devices Help</th> <th></th>	File Machine View	Input Devices Help	
Image: Construction	V	Internet Information Services (IIS) Manager	_ 0 X
File View Help Concetors Create Self-Signed Certificate WIN-VU7/U9/GWTO(W Specify Friendly Name Specify a file name for the certificate request. This information can be sent to a certificate authority for signing: Specify a file name for the certificate: Erel Specify a file name for the certificate: Erel S	€ 💿 🖣 🖌 WIN-VJ70	JU9G4VTO >	🖸 🛛 🔄 🕡 -
Connections Actions Create Self-Signed Certificate Page Specify Friendly Name Specify a file name for the certificate request. This information can be sent to a certificate authority for signing: Specify a file name for the certificate: Specify a file name for the new certificate: Specify a file name for the new certificate: Select a certificate store for the new certificate: Select a certificate: Select a certificate store for the new certificate: Select a certificate store for the new certificate: Select a certificate store for the new certificate: Select a certificate	File View Help		
Set Page Specify Friendly Name Specify Friendly Name Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate request. This information can be sent to a certificate authority for againg. Specify a fle name for the certificate. Personal OK Cancel OK Cancel Image: Content View Reduce View Content View Reduce Vie	Connections	Act	tions
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing: Specify a file name for the certificate request. This information can be sent to a certificate authority for signing: Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate Request. Specify a file name for the certificate request. This information can be sent to a certificate authority for served Certificate authority for served Certificate Request. Specify a file name for the certificate served Certificate authority for served Certificate authority for served Certif	🔍 - 🔡 🖄 😹	Create Self-Signed Certificate ? ×	mport
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing: Specify a file name for the certificate request. This information can be sent to a certificate authority for signing: Specify a file name for the certificate: Lest Select a certificate store for the new certificate: Personal OK Cancel Cancel Second Cancel Second Cancel Second		Specify Friendly Name	Create Certificate Request Complete Certificate Request Create Domain Certificate
Specify a friendly name for the certificate: Select a certificate store for the new certificate: Personal OK Cancel	, pres	Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:	Create Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate
Select a certificate store for the new certificate Personal OK Cancel C III Personal C III Personal C III C III Personal C III C IIII C IIIII C IIIII C IIIII C IIIII C IIIII C IIIII C IIIII C IIIII C IIIIII C IIIII C IIIIII C IIIIII C IIIIIII C IIIIIII C IIIIIIIII C IIIIIIIIII		Specify a friendly name for the certificate: test	Help
Cancel C III >> C IIII >> C III >> C IIII >> C III >> C IIII		Select a certificate store for the new certificate: Personal	
CK Cancel			
CK Cancel CK Content View Ready Content View CK Conten			
Image: Content View			
K III > K III > Image: Second s	2	OK Cancel	
Image: Second		< <u> </u>	
Ready 9 Image: Constraint of the second secon	<	> 🔚 Features View 🖓 Content View	
	Ready		9

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

Windows Server 2012 R2 (HTTPS Yapıldıktan Sonra) [Running] - Oracle VM VirtualBo	x •••
File Machine View Input Devices Help	
Internet Information Services (IIS) Manager	
(ⓒ) ♥ WIN-VJ/UU9G4V10 → Sites → Default Web Site →	
File View Help	
Connections Image: Start Page Image: Start Page	Actions Explore Edit Permissions Edit Site Bindings Basic Setings View Applications View Virtual Directories Manage Website Restart Start Stop Browse Website Browse Website Browse Website Browse ":80 (http) Browse ":80 (http) Rowse ":443 (https) Advanced Settings Configure Limits Help
Ready	
	19:39
	16.7.2021

- Açılan ekranda sağ sütundaki "Bindings" etiklanır.



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

v	Vindows Server 2012 R2 (HTTPS Yapıldıktan Sonra) [Running] - Oracle VM VirtualBox	
File Machine View Input	Devices Help	
V	Internet Information Services (IIS) Manager	_ 0 ×
(€) (€) (€) (€) (€) (€) (€) (€) (€) (€)	FO → Sites → Default Web Site →	🔛 🖂 🔐 -
File View Help		
Connections		Actions
· 🔍 - 🔚 🖄 😪	Default Web Site Home	A Explore
📲 Start Page	Filter T Go - Go Show All Group by: Area	Edit Permissions
MIN-VJ7UU9G4VTO (WIN-VJ7UU		Edit Site
⊿ Sites	Site Bindings ? 🗙	Bindings
Default Web Site	Edit Site Binding ? X	Basic Settings
	Type	View Applications
i) 🛛 🖓	Type: IP address: Port:	View Virtual Directories
	https v All Unassigned v 443	anage Website 🕥
	Host name:	Restart
	a .	Stop
	Require Server Name Indication	Browse Website
	••	Browse *:80 (http)
	SSI certificate	Browse *:443 (https)
iii) —	test V Salart View	Advanced Settings
/	View	Configure
		Limits
	OK Cancel) Help
< 111	> Features View Content View	
Ready		G
		19:41
		🖓 🖾 🖉 🔘 🐼 💽 Right Ctrl

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

Activities	Common	
9		
Web Sizma Testleri	Windows Server 2012 R2 (HTTPS Yapıldıktan Sonra) [Running] - Oracle VM VirtualB	••× 🛛 🖓 🖓
🐸 🗛 🛛 IIS Windows Server - Chromium 🛛 🔘 🕲	Ingernet Information Services (IIS) Manager	- 6 X
🕎 📀 IIS Windows Server X + 📀 IIS Windows Server X +		□ ≥ 0 10 •
← → C ☆ ▲ Not secure https://192.168.0.29 第 ☆ 0 �a ★ ≗	E File View Help	
🔛 📰 Apps 🗶 İş Gücü Girişi 💠 Jir Gücü 🗶 Confluence SGE 🛽 Log in to bya	Connections Default Web Site Home	Actions
	Billing Start Page	Edit Permissions
Windows Server	A MIN-V/7UU9G4/TO (WIN-V/7UU9G4/ Application Pools IIS	Edit Site
	A 🐼 Sites 💦 🧐 🚡 📰 🔝 🗐	Basic Settings
E Internet Information Services	Pu: Authenticati Compression Default Directory Error Pages Handler on Document Browsing Mappings	View Applications View Virtual Directories
	📲 📲 🏓 🍻 着	Manage Website 💿
	HTTP Logging MIME Types Modules Output Request Respon Caching Filtering	Start
		E Stop
	SSL Settings	Browse Website Browse *:80 (http)
	Manager	Browse *:443 (https)
Welcome Bienvenue Tervetuloa		Advanced Settings
	GU Configurat	Limits
ようこそ Benven to 歌迎	Editor	😧 Help
🕒 🛑 אים הבאים Bienvenido Hoş geldiniz אים הבאים אים 📔		
Bem-vindo		
🤗 🔤 Καλώς		
Viteite 00i00TE Välkommen 화영화니	K K	61
		60 De de 90 1952
Mutilidae Video		16.7.2021
Serisi.txt		
Lowservers		
Trash includekara smartasp Pl buk Bilgil tuzlucavir	hpMyAdm	
login bilg A	uth Cre Belgeleri	

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_SHA256 (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,

 $\label{eq:hkey_local_machine} Key_local_machine System \currentControlSet \controlSecurityProviders \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.

1	Windows S	erver 2012 R2 (HTTPS Yapıldıl	ktan S	onra) [Running] -	Oracle VM Virtu	JalBox		000
File Machine View	Input Devices	Help						
V ij	R	Internet Informatio	n Serv	ices (IIS) Manager				_ 0 ×
🛞 💮 😜 🖌 WIN-V	/J7UU9G4VTO Sites	Default Web Site					1	📴 🖂 🔛 🕶
File View Help								
Connections							Actions	
🔍 - 🗔 🖄 🔗		Default Web Site Hor	ne				A Explore	
💐 Start Page	Fil	ter T Go v la	Show	All Group by: Area	· 💷 ·		Edit Permiss	ions
⊿ ♥ WIN-VJ7UU9G4VTO (ANNI WERHOCALD		Renist	v Editor	· [22] ·		- 🗆 X	
Application Pools	Eile Edit View En	voriter Help	tegisti	y Editor		L		
👂 😔 Default Web S		ProductOptions		Name	Type	Data		
	▶-	SafeBoot		(Default)	REG_SZ	(value r	not set)	tions
	-	ScEvents		👪 Enabled	REG_DWORD	0x00000	0000 (0)	hirectories
	D **	ScsiPort						۲
	Þ	SecurePipeServers						
	⊿ -	SecurityProviders						
		Ciphers						http)
								(https)
								tings
		⊿ - 🎉 Protocols						
		⊳ - 📔 SSL 2.0	≡					
		A SSL 3.0						
		TLS 1.0						
		TLS 1.1						
	-							
		ServiceGroupOrder						
		ServiceProvider	~	<	Ш		>	
Computer\HKEY_LOCAL_MACHINE\SYSTEM.CurrentControlSet\ControlNecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server								
< III > E Features View & Content View								
Ready								
		B					10 Rs (s	20:12
					S O B	U 🗗 🖉 (Right Ctrl

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:

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) 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) - Á TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C compressors: NÛLL cipher preference: server

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).

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 \Security Providers \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).



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				- 🗆 ×
IIS C	Crypto 3.2			SOFTWARE
Schannel	Schannel These settings enable or disable v default for the operating system of	arious options system wide. When vill be used. Click the Apply buttor	the checkbox is grey it means no se n to save changes.	tting has been specified and the
0	Server Protocols	Ciphers	Hashes	Key Exchanges
Cipher Suites	Multi-Protocol Unified Hello PCT 1.0 SSL 2.0	 ✓ NULL ✓ DES 56/56 ✓ RC2 40/128 ✓ RC5 56/120 	MD5 SHA SHA 256	Diffie-Hellman PKCS ECDH
Advanced	SSL 5.0 TLS 1.0 TLS 1.1 TLS 1.2	RC2 36/128 RC2 128/128 RC4 40/128 RC4 56/128	SHA 504	
		 RC4 64/128 RC4 128/128 Triple DES 168 AES 128/128 		
Templates		AES 256/256		
Site Scanner	Client Protocols Multi-Protocol Unified Hello PCT 1.0 SSL 2.0 CONTRACTOR			
About	SSL 3.0 TLS 1.0 TLS 1.1 TLS 1.2			

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.

🛃 IIS Crypto				– 🗆 X
📕 IIS (Crypto 3.2			SOFTWARE
Schannel	Schannel These settings enable or disable v default for the operating system	various options system wide. When t will be used. Click the Apply button	he checkbox is grey it means no se to save changes.	tting has been specified and the
Cipher Suites Cipher Suites Advanced	Server Protocols Multi-Protocol Unified Hello PCT 1.0 SSL 2.0 SSL 3.0 TLS 1.0 TLS 1.1 TLS 1.1 TLS 1.2	Ciphers NULL DE5 56/56 RC2 40/128 RC2 56/128 RC2 128/128 RC4 40/128 RC4 61/128 RC4 64/128 Triple DE5 168 AES 128/128 AES 128/128	Hashes MD5 SHA SHA 256 SHA 384 SHA 512	Key Exchanges Diffie-Hellman PKCS ECDH
Site Scanner	Client Protocols Multi-Protocol Unified Helto PCT 1.0 SSL 2.0 SSL 3.0 TLS 1.0 TLS 1.1 V TLS 1.2			

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-enumciphers denetlemesi yapılmıştır. Ardından ayarlamalar yapılıp reboot yapıldığında nmap ssl-enumciphers 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