

Parametre Analiz Kodu Test Senaryoları:

1. Önerilen değerini küçült.

ilk hal / Önerilen değer:1

security_analysis_report. xlsx:

3	rsau/enable	0	0		1 LOW	parametreyi yapması gereken kullanıcı parametresine uygun loglama yapılarak benzersiz dosya adlandırma kuralları oluşturulur.
4	rsau/max_dikenasa/local	1000000000	1000000000	>=100M	DIFFERENT	0 olarak ayarlanırsa loglama yapılmaz ve olay sonrası analiz imkânsızlaşır. Kullanıcının yapması gereken: Değeri 1 olarak ayarlayarak loglamayı aktif hale getirin.

ikinci hal / Önerilen değer:0

security_analysis_report. xlsx:

3	rsau/enable	0	0		0 SAME	kuralları oluşturulur.
4	rsau/max_dikenasa/local	1000000000	1000000000	>=100M	DIFFERENT	Güvenlik denetim loglaması aktiftir. Çok yüksek değerler dikkat edilmesi ve

2. Önerilen değerini büyüt.

ilk hal / Önerilen değer:0

security_analysis_report. xlsx:

49	itsp/enable	1	1	aktif	0 HIGH	parametre SAP sisteminde bulunmadığı - status: NOT_FOUND
50	itsp/diagnostic_saf	0	0		1 LOW	1 olarak ayarlanırsa gereksiz bir hizmet açık kalır ve saldırı yüzeyi artar. Kullanıcının yapması gereken: ITS protokolünü devre dışı bırakmak için değeri 0 olarak ayarlayın.

ikinci hal / Önerilen değer: 2

security_analysis_report. xlsx:

49	itsp/enable	1	1		2 LOW	NOT_FOUND
50	login/disable_cplic	0	0		1 LOW	ITS protokolünü devre dışı bırakmak için değeri 0 olarak ayarlayın.

3. Önerilen değeri Current value ile aynı yap.

ilk hal / Önerilen değer :1

security_analysis_report. xlsx:

65	login/ticket_only_to_host	0	0		1 LOW	0 ise ticket başka sistemlerde de kullanılabilir. Kullanıcının yapması gereken: Değeri 1 olarak ayarlayarak ticket'in sadece oluşturulduğu host'a geçerli olmasını sağlayın.
----	---------------------------	---	---	--	-------	--

ikinci hal / Önerilen değer: 0

security_analysis_report. xlsx:

65	login/ticket_only_to_host	0	0		0 SAME	Oturum bileti sadece belirli host'a geçerlidir.
----	---------------------------	---	---	--	--------	---

4. Sahte Parametre: Excel'e olmayan bir parametre ekle.

parametreler.xlsx :

122				ve güncel bir kütüphane	çinli olur.	
123	deneme	1		yolunu işaretlediğinden emin olun.	değer yüksekse / farklıysa	değer aynıysa
124				değer düşükse		
125						

Excel e eklediğim ama olmayan parametreyi (deneme) bulamadı ve uyarı mesajı verdi.

```
Parametre analiz ediliyor: ssf3/ssfapi_lib
Parametre analiz ediliyor: deneme
UYARI: Parametre bulunamadı: deneme
SAP bağlantısı kapatıldı. 110 parametre başarıyla çekildi.
Bulunamayan parametreler: ['auth/system_access_check_off', 'rfc/ext_debugging', 'gw/tcp_security', 'icm/serverport', 'is/HTTP/virhost', 'is/SMTP/virhost', 'login/password_compliance_to_current_policy', 'ms/serverport', 'rdisp/auth_check_user_list', 'snc/permit_comm', 'snc/permit_insecure_comm', 'deneme']

122 güvenlik parametresi SAP'den işlendi

Güvenlik analizi başlıyor...
Güvenlik veritabanında 122 parametre tanımlı yüklendi

GÜVENLİK ANALİZ RAPORU:
Toplam analiz edilen parametre: 122
Bulunamayan parametreler: 108
Bulunamayan parametreler: 11
```

Bulunamayan parametrelerin hepsini tek tek denedim ve onlar (aşağıdaki resimlerdeki gibi) sistemde yoklar. Belki eskimişlerdir ve kullanılmıyorlardır artık veya tanımlı değildir diye düşünüyorum.

Profile Parameter Maintenance

Parametername

auth/system_access_check_off

Display

Display docu

☒ The parameter name is not known

☒ The parameter name is not known

Profile Parameter Maintenance

Parametername

rfc/ext_debugging

Display

Display docu

☒ The parameter name is not known

☒ The parameter name is not known

NOT:

9	auth/authorization_trace			active	INCOMPLETE_DATA	Parametre değeri veya önerilen değeri eksik - manuel kontrol gerekli
---	--------------------------	--	--	--------	-----------------	--

INCOMPLETE_DATA olarak gösterdiği bütün parametreler gui de aşağıdaki gibi gözüküyorlar.

Metadata for Parameter auth/authorization_trace	
Description	Value
Name	auth/authorization_trace
Type	String
Further Selection Criteria	{Y y N n F f } {0,1}
Unit	
Parameter Group	Auth
Parameter Description	Trace every authority-check once for authorization proposals
CSN Component	BC-SEC-AUT-PFC
System-Wide Parameter	No
Dynamic Parameter	Yes
Vector Parameter	No
Has Subparameters	No
Check Function Exists	No
Value of Profile Parameter auth/authorization_trace	
Expansion Level	Value
Kernel Default	
Default Profile	
Instance Profile	
Current Value	
Origin of Current Value: Kernel Default	

Kodun Genel Özeti

Bu script, bir **SAP sistemi üzerindeki güvenlik parametrelerini otomatize bir şekilde analiz etmek** için tasarlanmıştır. Temel amacı, parametreler.xlsx adında bir Excel dosyasında listelenen kritik güvenlik parametrelerinin SAP sistemindeki mevcut değerlerini çekmek, bu değerleri yine aynı Excel dosyasında belirtilen **önerilen değerlerle** karşılaştırmak ve sonuçları security_analysis_report.xlsx adında detaylı bir rapora dönüştürmektir.

1. Başlatma ve Hazırlık

- Script ilk olarak parametreler.xlsx dosyasını okur. Buradan hangi SAP parametrelerini denetleyeceğini öğrenir.
- Ardından kullanıcının bilgisayarındaki SAP Logon programını çalıştırır ve belirtilen SAP sistemine (kullanıcı adı, şifre gibi bilgilerle) otomatik olarak bağlanır.

2. SAP'den Veri Çekme (sap_connect_and_extract fonksiyonu)

- SAP sistemine giriş yaptıktan sonra, SA38 işlem kodunu çalıştırır ve RSPARAM raporunu açar. Bu rapor, sistemdeki tüm parametreleri ve değerlerini gösterir.
- Excel'den aldığı parametre listesindeki her bir parametre için RSPARAM raporunda tek tek arama yapar.
- Arama sonucunda bulduğu parametrenin **mevcut değerini, sistem varsayılan değerini ve kullanıcı tarafından atanmış değeri** okur.
- Eğer bir parametreyi bulamazsa, bunu not eder.
- Tüm parametreler için bu işlemi tamamladıktan sonra topladığı ham verileri bir liste halinde hazırlar ve SAP bağlantısını kapatır.

3. Güvenlik Analizi ve Karşılaştırma (security_advice_engine fonksiyonu)

- Bu aşama, script'in "beyni" olarak düşünülebilir. SAP'den gelen ham veriyi alır.
- Tekrar parametreler.xlsx dosyasını okur. Ancak bu sefer her parametre için belirlenmiş **"Önerilen Değer"** ve bu değere uyulmadığında verilmesi gereken **"Tavsiye"** metinlerini alır.
- SAP'den gelen her bir parametrenin mevcut değerini, olması gereken önerilen değer ile karşılaştırır.

4. Değerlendirme Mantığı (analyze_security_parameter fonksiyonu)

- Karşılaştırma işlemi sırasında basit bir mantık izler:
 - **Sayısal Değerler:** Eğer değerler sayı ise (örneğin, login/fails_to_user_lock = 3), mevcut değer önerilen değerden büyük, küçük veya eşit olup olmadığını kontrol eder.
 - **Metinsel Değerler:** Eğer değerler metin ise (örneğin, TRUE veya FALSE), mevcut değer önerilenle aynı olup olmadığını kontrol eder.
- Bu karşılaştırmanın sonucuna göre parametrenin durumunu belirler: **SAME** (Aynı), **HIGH** (Yüksek), **LOW** (Düşük) veya **DIFFERENT** (Farklı).

5. Raporlama

- Son olarak, toplanan tüm bilgileri (parametrenin adı, mevcut değeri, önerilen değeri, karşılaştırma durumu ve güvenlik tavsiyesi) düzenli bir şekilde bir araya getirir.

- Bu bilgileri security_analysis_report.xlsx adında yeni bir Excel dosyasına yazdırır. Bu rapor, denetimin nihai çıktısıdır ve hangi parametrelerin riskli olduğunu ve ne yapılması gerektiğini açıkça gösterir.