

OTURUM AÇMA TÜRÜ

Windows Oturum Açma Türleri ve SOC Analistine nasıl katkıda bulundukları.

Bir kullanıcı ve bir makine arasındaki etkileşim nasıl başlar?

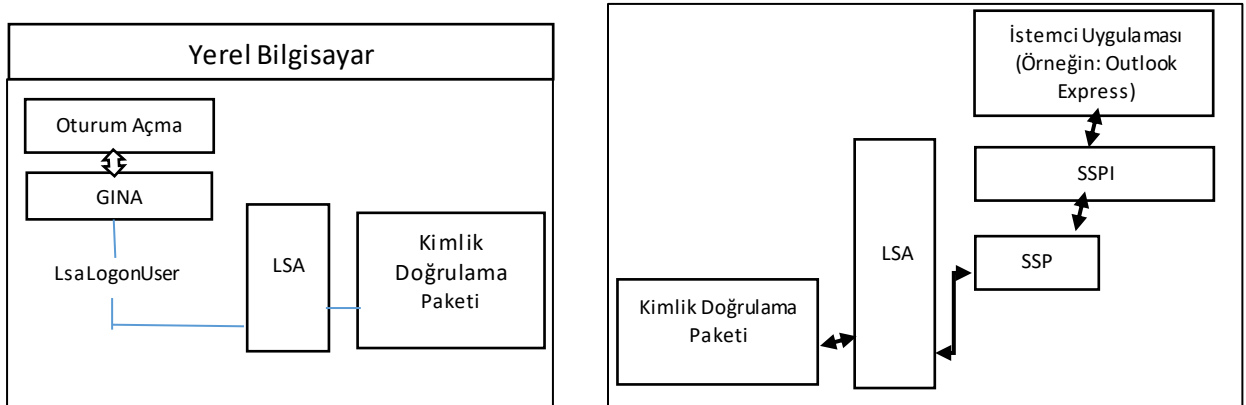
Kullanıcının başarılı veya başarısız oturum açması hakkındaki bilgimize eklenen birkaç Windows LOGON türü vardır.

Logon tipine sahip olduğumuzda, kullanıcının bilgisayarın önünde mi yoksa uzaktan mı bağlı olduğunu, kaydetme ekranının kilidini mi açtığını veya bir insan değil de bir hizmet olabilir mi, bilebiliriz.

SOC Analistine nasıl yardımcı olabilir?

Kullanıcının nasıl bağlantı kurduğunu bilmek, şüpheli Oturum Açmaları iyi niyetli oturumlardan ayırmamız için bize bir araç sağlar.

ETKİLEŞİMLİ OTURUM AÇMA ve İNTERAKTİF OLMAYAN OTURUM AÇMA



- Type 2 – Etkileşimli
- Type 3 – Ağ
- Type 7 – Kilidi Aç
- Type 10 – Uzak Etkileşimli (Terminal hizmetleri, Uzak Masaüstü Hizmetleri)

Etkileşimli oturum açma işlemi, bir kullanıcı kimlik bilgileri giriş iletişim kutusuna kimlik bilgilerini girdiğinde veya kullanıcı akıllı kart okuyucusuna bir akıllı kart taktığında veya kullanıcı bir biyometrik cihazla etkileşim kurduğunda başlar. Kullanıcılar, bir bilgisayarda oturum açmak için yerel bir kullanıcı hesabı veya bir etki alanı hesabı kullanarak etkileşimli bir oturum açabilir. Etkileşimli olmayan kullanıcı Oturum Açma işlemi, bir kullanıcı adına bir istemci uygulaması veya bir işletim sistemi bileşeni tarafından gerçekleştirilir. Bu Oturum Açmalar, kullanıcının bir Kimlik Doğrulama faktörü sağlamasını gerektirmez. Bunun yerine, cihaz veya istemci uygulaması, bir kullanıcı adına bir kaynağa kimlik doğrulaması yapmak veya bu kaynağa erişmek için bir belirteç veya kod kullanır. Bu oturum açmalar, kullanıcının etkinliğinin arka planında gerçekleşir. Etki alanı oturum açma - hesap adı ve

parola veya sertifika gibi yerel oturum açma için gerekli öğeleri ve Active Directory etki alanı bilgilerini birleştirir.

GINA Grafik Tanımlama ve Kimlik Doğrulama (DLL). Winlogon tarafından yüklenir, etkileşimli oturum açma modelinin kimlik doğrulama politikasını uygular, tüm tanımlama ve kimlik doğrulama kullanıcı etkileşimlerini gerçekleştirir

ETKİLEŞİMLİ OLMAYAN OTURUM AÇMA ÖRNEKLERİ

- Bir istemci uygulaması, erişim belirteci almak için bir OAuth 2.0 yenileme belirteci kullanır.
- Bir istemci, erişim belirteci almak ve belirteci yenilemek için bir OAuth 2.0 yetkilendirme kodu kullanır.
- Kullanıcı, Azure AD'ye katılmış bir bilgisayarda bir web veya Windows uygulamasında çoklu oturum açma (SSO) gerçekleştirir.
- Bir kullanıcı, FOCI (Müşteri Kimlikleri Ailesi) kullanarak bir mobil cihazda oturumu varken ikinci bir Microsoft Office uygulamasında oturum açar.
- SolarWinds araştırması sırasında, Microsoft Araştırmaları, kötü niyetli aktörün “Veri Erişimi” elde etmek için hassas bir uygulama kullanıp kullanmadığını kontrol ettiğinde, Tehdit Avcılığı sürecinde bir dal vardı.

Hizmet sorumlusu ve uygulama kimlik bilgilerinin oluşturulmasını ve kullanımını denetleyin. Sparrow, bu kimlik bilgilerindeki değişiklikleri algılayacaktır. Etkin olmayan veya unutulmuş uygulamaların yeniden kullanılması gibi olağandışı uygulama kullanımına bakın. Uygulama tarafından etkileşimli olmayan oturum açmaya izin veren uygulamalara kimlik bilgilerinin atanmasını denetleyin. Azure AD'ye eklenen beklenmeyen güven ilişkilerini arayın.

OTURUM AÇMA SÜREÇLERİ

Bir Windows günlüğündeki Oturum Açma İşlemi alanı, kullanıcının sisteme nasıl erişmeye çalıştığına dair bir ipucu sağlar: konsolunda, Sunucu İletim Bloğu (SMB - paylaşılan dosyalar için) veya Ortak İnternet Dosya Sistemi (CIFS - paylaşılan sağlamak için kullanılan ağ dosya sistemi protokolü) dosyalara ve yazıcılara erişim) paylaşılan klasör erişimi için veya IIS aracılığıyla. Bazı oturum açma işlemleri, aşağıdaki çizelgede gösterildiği gibi, kimlik doğrulama protokolüne özgüdür.

Process (İşlem)	Explanation (Açıklama)
Winlogon	Windows Oturum Açma İşlemi
Schannel (Kanal)	SSL, TLS gibi güvenli bağlantı.
İkinci Oturum Açma Hizmeti	(runas) - SecLogo
IKE	İnternet Anahtar Değişim protokol süreci.
Advapi	Web tabanlı oturum açma: IIS oturum açma işlemleri.
PKU2U	User-2-User Açık Anahtar Kriptografisi.
Kerberos	Bilet tabanlı, güvenli olmayan ağ, etki alanı üzerinde güvenli düğüm iletişimi için.
NtLmSsp	NT Lan Yöneticisi Hash tabanlı – Yerel olarak kullanılır.

GÜVENLİK DESTEĞİ SAĞLAYICILARI – SSP

SSP, güvenlik doğrulaması yapan bir yazılım modülüdür.

Negotiate – SSPI (arayüz) ve diğer SSP arasında uygulama katmanı görevi gören SSP. Bir uygulama bir Ağda oturum açmak için SSPI'yi aradığında, Müşteri tarafından yapılandırılan güvenlik ilkesine dayalı olarak isteği işlemek için en iyi SSP'yi seçebilen Anlaşma'yı çağırır.

KERBEROS protokolü güvenlik paketi - endüstri standardı güvenlik paketi. 3 bölümden oluşur: 2 bileşenli İstemci, Sunucu ve Anahtar Dağıtım Merkezi: Kimlik doğrulama hizmeti ve Bilet verme-Bilet hizmeti.

NTLM Güvenlik Paketi - Bu, NTLM (NT (Yeni Teknoloji) LAN Yöneticisi) ağları için birincil güvenlik paketi. Hash'leri kullanır. İki bölüm: İstemci ve Ana Bilgisayar. Bir Ağ üzerinden gönderilen oluşturulan karmalarla çalışır.

SCHANNEL SSP - SSL, özel iletişim teknolojisi (PCT) ve aktarım düzeyi güvenliğini (TLS) tek bir güvenlik paketinde birleştiren Microsoft Birleşik Protokol Sağlayıcı güvenlik paketini uygular. Schannel, öncelikle güvenli Köprü Metni Aktarım Protokolü (HTTP) iletişimlerini gerektiren İnternet uygulamaları için kullanılır.

WDIGEST - LDAP ve web tabanlı kimlik doğrulama için öncelikle Windows Server 2003'te kullanılan bir sorgulama/yanıt protokolü. Kimlik doğrulaması için Köprü Metni Aktarım Protokolü (HTTP) ve Basit Kimlik Doğrulama Güvenlik Katmanı (SASL) alışverişlerini kullanır.

OTURUM TÜRLERİ

Logon Type 2 – Etkileşimli

Bu sadece yerel bir bilgisayarda oturum açmak, kullanıcı adı ve parola yazmaktır. Kullanıcı yerel veya etki alanı hesabıyla oturum açar. Bu oturum açma türü yalnızca, bir kullanıcı etki alanında gerçekten kimliği doğrulandığında (bir etki alanı denetleyicisi tarafından) görünür. DC'nin mevcut olmaması, ancak kullanıcının yerel PC'de ön belleğe alınmış geçerli etki alanı kimlik bilgilerini onaylaması durumunda, Windows oturum açma türü = 11 (CachedInteractive) olan bir olayı günlüğe kaydeder.

Authenticators: Password, Smartcard

- Yerel oturum açma, bir kullanıcıya yerel bilgisayardaki Windows kaynaklarına erişme izni verir.
- Yerel oturum açma, kullanıcının yerel bilgisayardaki Güvenlik Hesapları Yöneticisi'nde (SAM) bir kullanıcı hesabına sahip olmasını gerektirir.

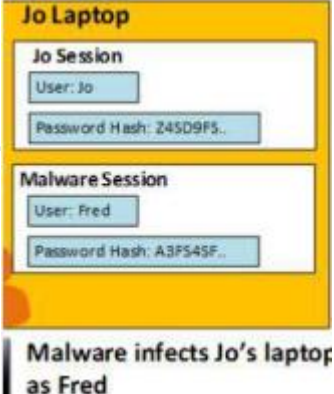
Logon Type 3 – Network

Ağdan bir bilgisayara erişildi. Çoğunlukla paylaşılan kaynaklara (paylaşılan klasörler gibi) ve yazıcılara bağlanma. Ağda oturum açma, bir kullanıcıya, kimlik bilgisinin erişim belirteciyle tanımlandığı şekilde, ağ bilgisayarlarındaki tüm kaynaklara ek olarak yerel bilgisayardaki Windows kaynaklarına erişme izni verir. Yalnızca yerel kimlik doğrulamasından sonra. İnternet Information Services (IIS) oturumlarının çoğu Tip 3'tür, istisna, Oturum Açma Türü 8'de açıklanan temel kimlik doğrulama. [IIS, bir Windows makinesine yerleştirilebilen bir web sitesi barındırma hizmeti olduğundan, Ağdan bir makineye erişmek gibidir] Doğrulamalar: Şifre, Kerberos ticket, NT Hash.

TESPİT ETME

Pass-the-Hash Detection: Bir ağdaki bir bilgisayar, uzak bir aktör tarafından ele geçirildikten sonra. PtH girişimlerinin yanal hareketi iş istasyonları arasında görülebilir:

- Microsoft Event Security Log ID 4624
 - LogonType 3 using NTLM
 - Event level information
 - Authentication is NOT a domain and NOT anonymous
 - Security ID is commonly null for PtH attacks



```
An account was successfully logged on.

Subject:
  Security ID:      S-1-0-0
  Account Name:     -
  Account Domain:   -
  Logon ID:         0x0

Logon Type:        3

Impersonation Level:  Impersonation

New Logon:
  Security ID:      -
  Account Name:     ANONYMOUS LOGON
  Account Domain:   NT AUTHORITY
  Logon ID:         -
  Logon GUID:       {00000000-0000-0000-0000-000000000000}

Process Information:
  Process ID:       0x0
  Process Name:     -

Network Information:
  Workstation Name:  ULV-000
  Source Network Address: 10.0.0.0.0
  Source Port:       56581

Detailed Authentication Information:
  Logon Process:     NtLmSsp
  Authentication Package: NTLM
  Transited Services: -
  Package Name (NTLM only): NTLM V1
  Key Length:        128
```

Olay Kimliği 4624 (Windows Olay Görüntüleyicisi'nde görüntülenir) , yerel bir bilgisayarda her başarılı oturum açma girişimini belgeler . Bu olay, erişilen bilgisayarda, başka bir deyişle, oturum açma oturumunun oluşturulduğu yerde oluşturulur. İlgili bir olay, Olay Kimliği 4625 belgeleri başarısız oturum açma girişimleridir.

Logon Type 4 – Batch

Bu, Zamanlanmış Görevler ile ilgilidir.

Windows bir zamanlanmış görevi yürüttüğünde, Zamanlanmış Görev hizmetleri, görev oluşturulduğunda belirtilen kullanıcı hesabının yetkisi altında çalışabilmesi için önce görev için yeni bir oturum açma oturumu oluşturur.

Oturum açma türü 4 olayları genellikle zararsızdır, ancak kötü niyetli bir kullanıcı, zamanlanmış görevler aracılığıyla bir hesabın parolasını tahmin etmeye çalışabilir. Bu tür girişimler, oturum açma türünün 4 olduğu bir oturum açma başarısız olayı oluşturur.

Ancak, zamanlanmış görevlerle ilişkili oturum açma hataları, bir yöneticinin görev oluşturma sırasında hesap için yanlış parola girmesinden veya zamanlanmış görevi yeni parolayı kullanacak şekilde değiştirmeden bir hesabın parolasının değiştirilmesinden de kaynaklanabilir.

Authenticators: Parola (genellikle LSA sırrı olarak saklanır). schtasks.exe ve at.exe (eski) ve bunların ana işlemlerini izlemeniz önerilir.

Logon Type 5 – Service

Her hizmet, belirtilen bir kullanıcı hesabı olarak çalışacak şekilde yapılandırılmıştır. Örnek: Tomcat9.exe'yi yönetici olarak çalıştırmak.

Bir hizmet başlatıldığında, Windows ilk olarak belirtilen kullanıcı hesabı için bir oturum açma oturumu oluşturur ve bu, oturum açma türü 5 olan bir olayla sonuçlanır. Ancak değişiklikler, Yönetici

haklarına sahip kötü niyetli kullanıcılar tarafından yapılabilir, çünkü yeni bir hizmet oluşturmak veya mevcut bir hizmeti düzenlemek için yüksek ayrıcalıklar gerekir.

Authenticators: Şifre (genellikle LSA sırrı olarak saklanır).

Logon Type 7 – Unlock

Kullanıcı bilgisayarını bir süreliğine terk ettiğinde, muhtemelen bilgisayarı kilitleyen ve böylece gözetimsiz iş istasyonunun kötü amaçlı kullanımdan korunmasını sağlayan bir ekran koruyucu vardır. Oturum açma türü 7, kullanıcı bilgisayarına geri döndüğünde ve kilidini açtığında gerçekleşir. Oturum açma türü 7 ile başarısız oturum açmalar, bir kullanıcının yanlış parola girdiğini veya kötü niyetli bir kullanıcının parolayı tahmin ederek bilgisayarın kilidini açmaya çalıştığını gösterir. Oturum açma türü 7 ile Dc'ye Başarılı Oturum Açmaları izliyoruz

Logon Type 8 – NetworkCleartext

Ağ oturum açma türü 3'e benzer, ancak burada parola ağ üzerinden açık metin olarak gönderildi. [Windows sunucusu, açık metin kimlik doğrulamasıyla paylaşılan dosyalara veya yazıcılara bağlantıya izin vermez.]

Bunlar, ADVAPI kullanılarak bir ASP betiği içinden veya bir kullanıcı IIS'nin temel kimlik doğrulama modunda oturum açtığında oturum açma işlemleri olabilir. Her iki durumda da, etkinliğin açıklamasındaki oturum açma işlemi advapi'yi listeleyecektir. Bir SSL oturumu (yani https) üzerinde değilse, temel kimlik doğrulama tehlikelidir. Parola, ASP betiğinde kaynak kodun içine gömülmeyecektir. Kötü niyetli birinin kaynak kodunu görüntülemesi ve parolayı alması riskinin yanı sıra bakım amacıyla kötü bir uygulamadır.

ADVAPI = Gelişmiş Windows 32 Base API, Advapi32.dll; güvenlik ve kayıt çağrılarını destekleyen bir API hizmetleri kitaplığıdır. advapi32.dll, yerel makine yöneticisi kullanıcısının Oturum açmasına izin veren bir belirteç içerir. Bu belirteç kopyalanabilir ve yerel makine yöneticisinin kimliğine bürünerek uzak kullanıcıların pencerelerde oturum açmasına izin vermek için kullanılabilir.



Logon Type 9 – NewCredentials

Farklı bir kullanıcı hesabı altında bir programı başlatmak için RunAs komutunu kullanmak ve /netonly anahtarını belirtmek, Windows'un bir oturum açma olay türü 9 kaydetmesine neden olur. Örnek: bir programı çalıştırın, ancak ağ bilgisayarları için ek izinler verin, kullanıcı Yöneticisini belirtin ve istendiğinde parolayı sağlayın. runas /netonly kullanmak, başka bir kullanıcıyla bir ağ üzerinden kimlik doğrulaması yaparken uygulamanızı yerel olarak sizin gibi çalıştırmanıza izin verir. /netonly olmadan Windows, programı yerel bilgisayarda ve ağda belirtilen kullanıcı olarak çalıştırır ve oturum açma olayını tip 2 olarak kaydeder.

Detection: PtH

Hash Saldırısını tespit etmeye yardımcı olabilir:

event ID: 4624

Logon process: Seclogon

Logon type: 9

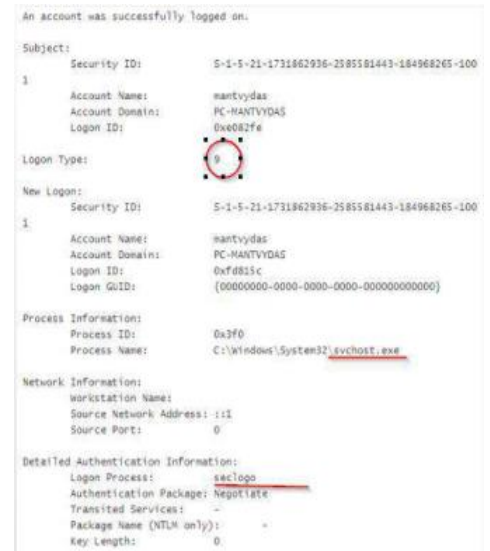
Authentication Package = Negotiate

Oturum açma türü 9, yeni süreçten kaynaklanan tüm ağ

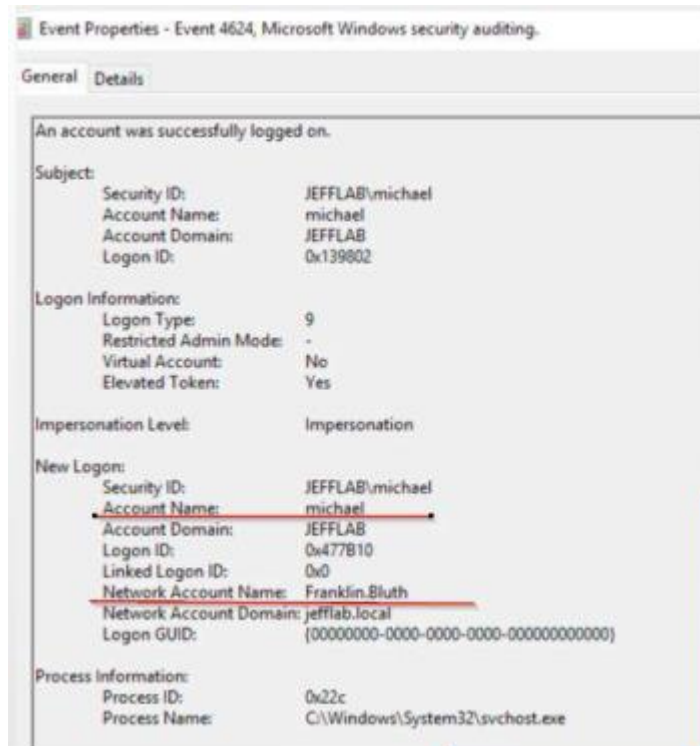
bağlantılarının yeni kimlik bilgilerini kullanacağı anlamına gelir.

Burada: user mantvydas bir komut çalıştırdı:

runas /user:low /netonly cmd =>



Başka bir örnek:

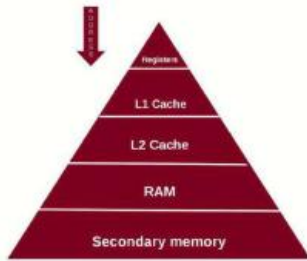


Logon Type 10 – RemoteInteractive

Bir bilgisayara Terminal Hizmetleri, Uzak Masaüstü veya Uzaktan Yardım aracılığıyla eriştiğinizde, Windows oturum açma girişimini oturum açma türü 10 ile günlüğe kaydeder. (XP'den önce Windows 2000, oturum açma türü 10 kullanmaz ve Terminal Hizmetleri oturum açma işlemleri, oturum açma türü 2 olarak bildirilir.)

Logon Type 11 – CachedInteractive

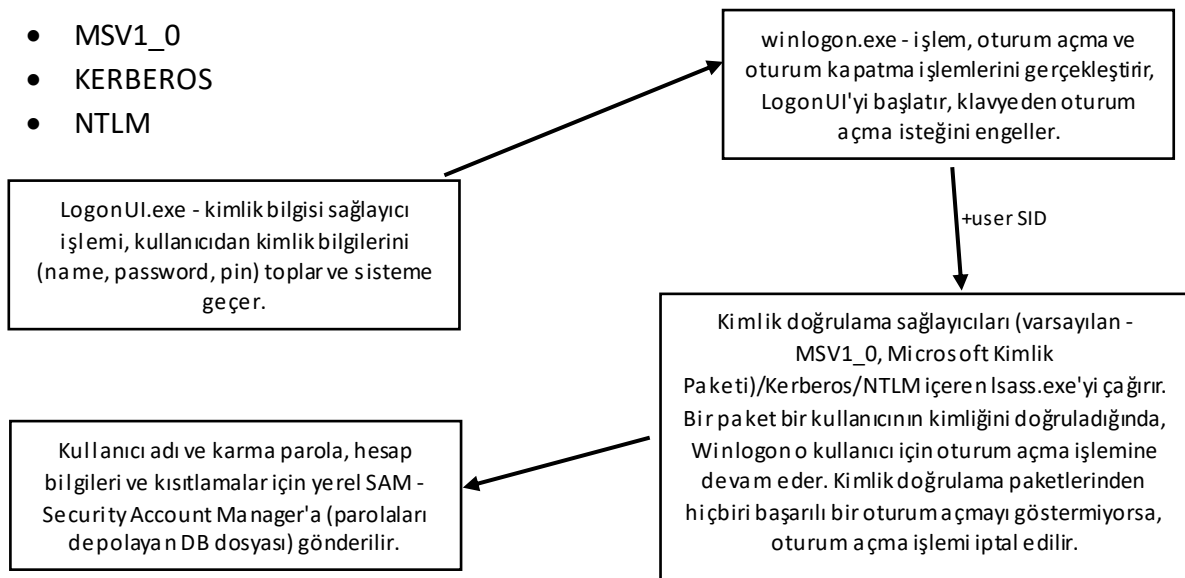
Windows, mobil kullanıcıları kolaylaştıran Önbelleğe Alınmış Oturum Açma adlı bir özelliği destekler. Kuruluşunuzun ağına bağlı olmadığınızda ve dizüstü bilgisayarınızda bir etki alanı hesabıyla oturum açmaya çalıştığınızda, dizüstü bilgisayarınızda kimliğinizi doğrulamak için kullanılabilir bir etki alanı denetleyicisi yoktur. Bu sorunu çözmek için Windows, son 10 etkileşimli etki alanı oturum açma işleminin kimlik bilgilerinin bir karmasını önbelleğe alır. Daha sonra kullanılabilir etki alanı denetleyicisi olmadığında, bir etki alanı hesabıyla oturum açmaya çalıştığınızda, Windows bu karmaları kimliğinizi doğrulamak için kullanır.



Başarısız giriş nedir?

Kimlik doğrulama paketleri, kimlik doğrulama kontrollerini gerçekleştiren DLL'lerdir.

- MSV1_0
- KERBEROS
- NTLM



SAM kısıtlamalarına örnek:



Lsass Başarısız oturum açma – Hatalı parola

C:\Windows\System32\lsass.exe	MICROSOFT_AUTHENTICATION_PACKAGE_V1_0	Advapi	Network
C:\Windows\System32\lsass.exe	MICROSOFT_AUTHENTICATION_PACKAGE_V1_0	Advapi	Network

Schannel Başarısız Oturum Açma Örneği

TLS1_ALERT_UNKNOWN_CA
48

SEC_E_UNTRUSTED_ROOT
0x80090325

Schannel errors in Event Viewer tend to be really unhelpful. From MSDN, Error 48 indicates TLS1_ALERT_UNKNOWN_CA SEC_E_UNTRUSTED_ROOT 0x80090325 so most likely due to a self-signed, or internal CA signed certificate on the host in question. But it doesn't indicate which client computer is triggering the error.

An account failed to log on.

Subject:

- Security ID: S-1-0-0
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

Account For Which Logon Failed:

- Security ID: S-1-0-0
- Account Name: -
- Account Domain: -

Failure Information:

- Failure Reason: An Error occurred during Logon.
- Status: 0xC000006D
- Sub Status: 0x80090325

Process Information:

- Caller Process ID: 0x0
- Caller Process Name: -

Network Information:

- Workstation Name: -
- Source Network Address: -
- Source Port: -

Detailed Authentication Information:

- Logon Process: Schannel
- Authentication Package: Microsoft Unified Security Protocol Provider
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

Bu bir SSL sorunudur ve istemci makineye dahili CA sertifikası eklenerek çözülebilir.

Diğer Uygulamalar: NegoExtender

NegoExtender AP - Uzantıları SSP'de Anlaşma (Negoexts.dll)

PKU2U - Genel Anahtar Şifreleme Kullanıcıdan Kullanıcıya, eşler arası

Bilgisayarlar, çevrimiçi kimlikler kullanılarak kimlik doğrulama isteklerini kabul edecek şekilde yapılandırıldığında, Negoexts.dll, oturum açmak için kullanılan bilgisayarda PKU2U

SSP'yi çağırır. PKU2U SSP, yerel bir sertifika alır ve politikayı eş bilgisayarlar arasında değiştirir. Eş bilgisayarda doğrulandığında, meta veriler içindeki sertifika, doğrulama için oturum açma eşine gönderilir. Kullanıcının sertifikasını bir güvenlik belirteciyle ilişkilendirir ve ardından oturum açma işlemi tamamlanır.

PKU2U kimlik doğrulamasında bir Ayrıcalık Yükselmesi (EoP) güvenlik açığı bulunmaktadır. Güvenlik açığından başarıyla yararlanan bir saldırgan, işlemleri yükseltilmiş bir bağlamda çalıştırabilir. Saldırganın güvenlik açığından yararlanabilmesi için önce sistemde oturum açması gerekir. (CVE-2021-25195, Kritik)

CLI kullanıcı girişi için Hyper-V'de kullanılabilir. Çevrimiçi kimliklerin etki alanına katılmış sistemlerde kimlik doğrulamasını önlemek için: Bilgisayar Yapılandırması >> Windows Ayarları >> Güvenlik Ayarları >> Yerel İlkeler >> Güvenlik Seçenekleri >> "Ağ güvenliği: Bu bilgisayara PKU2U kimlik doğrulama isteklerinin kullanılmasına izin ver için ilke değerini yapılandırın çevrimiçi kimlikler"den "Devre Dışı"ya.

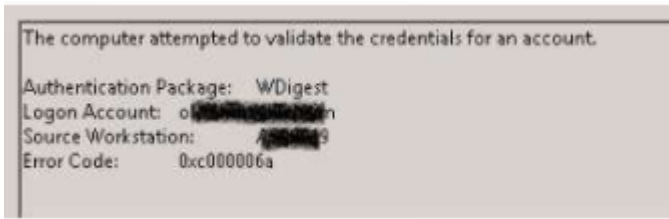
Diğer Uygulamalar: WDigest

Rare SSP – müşterilerimizin günlüklerinde bulunamadı.

WDigest Kimlik Doğrulaması, LDAP ve web tabanlı kimlik doğrulama için kullanılan bir sorgulama/yanıt protokolüdür.

Bir istemci erişim ister, kimlik doğrulama sunucusu istemciye meydan okur ve istemci, yanıtını paroladan türetilen bir anahtarla şifreleyerek yanıt verir. Şifrelenmiş yanıt, kullanıcının doğru parolaya sahip olup olmadığını belirlemek için kimlik doğrulama sunucusunda saklanan bir yanıtla karşılaştırılır.

WDigest, parolaları düz metin olarak bellekte saklar. Kötü niyetli bir kullanıcının bir uç noktaya erişimi varsa ve Mimikatz gibi bir aracı çalıştırabiliyorsa, yalnızca o anda bellekte depolanan karmaları almakla kalmaz, aynı zamanda hesaplar için düz metin şifresini de alabilirler.



Event ID 4624

'Authentication Package: WDigest