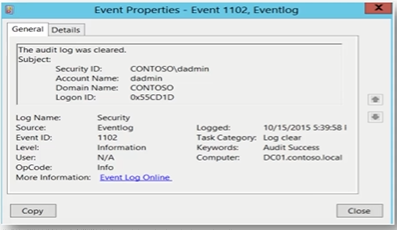
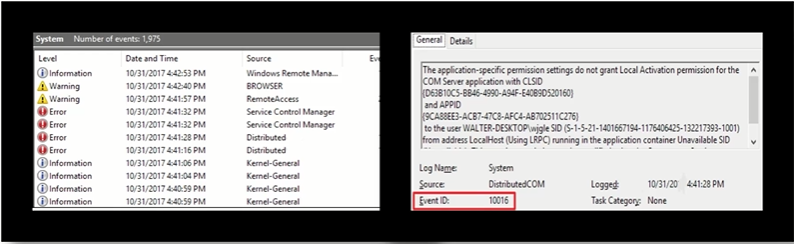
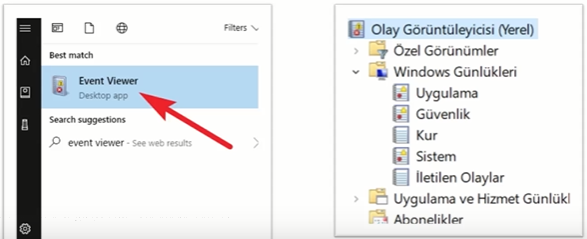
**Loglama Yönetimi Ve Analizi**  
Windows işletim sistemlerde log kayıtlarının tutulduğu yere olay günlükleri (event log) denir. Sistemde gerçekleşen tüm hareketler kayıt altına alınır.  
**Windows Event Viewer(Olay Görüntüleyicisi)**hatalar ,bilgi mesajları ve uyarılar da dahil olmak üzere uygulama ve sistem mesajlarının bir kaydını gösterir.Her türlü Windows sorununu gidermek için kullanışlı bir araçtır.  
Olay Görüntüleyici başlatmak için **Başlata** basın,arama kutusuna **“Olay Görüntüleyici”** veya **“Event Viewer”** yazın ve ardından çıkan arama sonucuna tıklayın.  
**Olay Görüntüleyici Kullanımları  
  
Windows Exchange Server Log İşlemleri**Exchange server log dosyaları siber saldırıları tespit etmek açsından önemlidir. Kullanıcılara gelen maillerin verilerine ulaşmak isteyen kullanıcıları ,mail trafiği bağlantı istekleri gibi bilgilerin yer aldığı loğlar analiz için oldukça önemlidir.  
**Wındows Event Loglar**   
**Event ID Nedir?**Olay günlüğü kayıt değerleri, Event ID olarak tanımlayabiliriz. Windows sistemlerde gerçekleşen işlemler neticesinde ciddi sayıda “Event ID” oluşmaktadır.  
**1102-log clearing**Sistemimizde audit log silindiğinde ilk oluşan loğdur ve oldukça önemlidir. Önemli olmasının en etkin sebebi ise istisnai durumlar dışında silinme ihtimalinin olmamasıdır.  
  
**Önemli Olay Kimliklerinden Bazıları  
4624-**Başarılı Login **4635-**Başarısız Login **4672-**Admin Hesabı Logini **4634,4647-**Başarılı Logoff  
**4771-**Etki alanında ön kimlik doğrulama başarısız oldu **4768-**Kerberos Ticket istemi  
**4776-**Etki alanında başarılı ya da başarısız login **7034-**Servis beklenmedik bir şekilde çöktü **7035-**Servis başlatma veya durdurma komutu gönderdi  
**7036-**Servis durdu veya başladı **7040-**Servis başlangıç tipi değiştirildi(Başlangıçta,elle,vs) **5140-**Ağ paylaşımı planlandı **4778-**RDP oturum isteği **4779-**RDP oturumu kapandı **Zamanlanmış Görevler  
106** Görev zamanlandı **200** Görev başlatıldı **201** Görev tamamlandı **141** Görev silindi



Windows içerisinde “zamanlanmış görev” loğları bilgisayarımızın ele geçirilip geçirilmediği hususunda bize fikir verebilir. Örneğin bir servisin günün belli saatlerinde oturum açılması için görev zamanlaması gerçekleştirilmesi şüpheli bir harekettir.  
  
**Windows Security (Güvenlik )Log Detayları**  
Sistem başlatılması kapatılması  
Sisteme yapılan başarılı ya da başarısız giriş işlemleri  
Hesap yönetimi ile ilgili işlemler  
Parola süresinin aşılması  
Bir dosyanın açılması  
İzin düzenlemeleri  
Domain düzenlemeleri  
Kullanıcı bilgilerinin düzenlenmesi  
Grup üyeliklerinin düzenlenmesi  
  
Windowsyüklü Server Saldırısı ve Log kayıtları  
Olay:Saldırganlar tarafından Windows server 2008 yüklü sunucuya “Hydra” aracı ile brute force saldırısı gerçekleştiriliyor.ve sonrasıda serverın (Adminstrator) şifresini bularak “Uzak masaüstü bağlantısı “ile sunucuya bağlanılıyor. Tüm bu aşamalarda oluşan event log kayıtlarını inceleyelim.

