06/03/2023-12/03/2023

Geçen hafta son olarak Windows Saldırı işlmlerine bakmıştım.Bu haftayı ise bu saldırıları önlemek için Windows sıkılaştırma işlemleri ne bakarak başladım.

Windows Sitemlerde Ağ Hizmetleri Sıkılaştırılması ,Windows Sistem ve Domain Sıkılaştırmaları, Windows Politika Prosedür ve Süreç İyileştirmelerine bakıldı.

Windows sıkılaştırma işlemleri , sistem güvenliğini arttırmak ve kötü amaçlı yazılımların veya saldırganların sisteme erişmesini zorlaştırmak için yapılan işlemlerdir.Ağ hizmetleri sıkılaştırması,ağ trafiğinin güvenliğini arttırmak için yapılan işlemlerdir.Sistem ve domain sıkılaştırmaları ise ,işletim sistemi ve domain yapısının güvenliğini arttırmak için yapılan işlmlerdir.Politika prosedür ve süreç iyileştirmeleri ise ,kullanıcıların sistem üzerindeki izilerinin düzenlenmesi ve gereksiz özelliklerin kapatılması gibi işlemler incelendi.

Daha sonra ileri seviye güvenlik gerektiren alanlar incelendi.Bunlardan ilki Güvenlik Duvarı (Firewall) ve loglama bu kısımda Firewallın görevleri öğrenildi.Firewall ile temel olarak neler yapılabileceği bilgisi (Erişim kontrolü,Kurallar oluşturma,Güncelleme ve yönetim) edinildi.Loglama ile ne tür kayıtlar tutabileceğimizi (Olay kayıtları,Raporlama,Alarm) bunların faydaları öğrenildi.

Önceki hafta Active Directory konusu incelenmişti bu hafta Active Directory İle yapılabilecek temel işlemler incelendi. Kullanıcı hesaplarını oluşturma silme ve yönetme, Grup politikalarını oluşturma ve yönetme,Verileri paylaşma,DNS yönetimi,Güvenlik izinlerini yönetme konuları Active Directory ile nasıl yapılabilir araştırılıp öğrenildi.

Active Directory'nin bir çok avantajı olmasına rağmen Okulumuz Bilgi İşlem Daire Başkanlığında bu hizmetin hem pahalılığı hem de yedekleme ve bakımda zahmetli olması sebebiyle kullanılmadığını öğrendim.

Daha sonar kuruma bazı görevler için yeni switchler gelmesi sebebiyle switchlerin çeşitlerini bu çeşitlerinin ne amaçla kullanıldığından ,hangi durumlarda hangi switchleri kullanmak gerektiğini öğrendim . Bir switch seçerken en önemli 3 kriterın ne olduğunu (peformans ,yönetilebilirlik.güvenlik) olduğunu öğrendim. Switchlerin artık 3.katmanda da çalıştığını burada da cpu ya ihtiyaç duyduğunu öğrendim.Support kavramını bir switche üretici firmanın kaç yıl desteği var ürün kalitesinin de önemli bir etken olduğunu öğrendim.Genel anlamda bir çok firmada Cisconun pahalılığı ve desteğinin az olması sebebiyle HP ve Dell marka switchlerin tercih edildiğini öğrendim.

Uğur TALAŞ hocamızdan Sql server eğitmi alındı. Okulumuz OBS veritabanı incelendi arka plandaki işleyiş öğrenildi.Okulumuz OBS veritabanının MSSQL ile yazıldığını ,bu kısımda tabloların birbiri ile bağlantısından,tablolardaki ortak verilerin ortak bir tabloda tutulduğundan,bir veritabanını yazmadan önce tasarlamanın öneminden, doğru tasarlanmadığı takdirde yazma kısmında büyük sorunlara yol açabileceğinden bahsedildi.Veritabanı yaklaşımları öğrenildi (Model-First,DBfirst,CodeFirst),HommerDB kavramından bahsedildi bu kavramın kötü amaçla kullanlabileceği öğrenildi.OBS veritabanında örnek sorgular denendi.Böylelikle gerçek bir veritabında işleyiş ile ilgili bilgi edinildi.Sistem performasnı için de okulumuz da karşılaşılan bir sorundan bahsedildi Server'ın 48 Core olmasına rağmen Database sürmü yüzünden tam performans alınamadığından bu yüzden system performansı için uygulamlarımızı yazdığımız editörlerin uyumuna dikkat etmemiz gerektiği vurgulandı.