Siber Güvenlik

Bazı Saldırı Türleri:

1-) XSS
2-) SQL Injection
3-) BruteForce
4-) Trojen
5-) RansomWare
6-) Phishing
7-) EVIL TWIN

Teknoloji insanların ihtiyaç ve isteklerini karşılamak üzere hedefe ulaşmak için kullanılan çevreyi geliştiren, değiştiren ve hatta dönüştüren bilgi, beceri, yöntem ve süreçlerinin tamamıdır.İnsanların ihtiyaçları doğrultusunda sürekli gelişmektedir ve bu gelişmeler doğrultusunda süreçler değişkenlik göstererek birtakım şeylerin önemi önplana çıkmıştır.Günümüzün en önemli varlığı verilerimiz olmuştur.Veriler kişi hakkındaki herhangi bir bilgi olabilir ve bunların yanlış kişilerin eline geçmesi halinde çok büyük sorunlar yaratabilecegini hepimiz biliyoruz.Bu verileri korumak ve gizliliğini sağlamak istedigimiz de Siber Güvenlik kavramına erişiyoruz.Küresel siber tehdit, her yıl sayısı artan veri ihlaliyle hızlı bir şekilde gelişmeye devam ediyor. RiskBased Security tarafından yayınlanan bir rapor, sadece 2019'un ilk dokuz ayında şaşırtıcı bir şekilde 7,9 milyar kaydın veri ihlallerine maruz kaldığını ortaya koydu. Bu rakam, 2018'in aynı döneminde ortaya çıkan kayıt sayısının iki katından (%112) fazla. Sağlık hizmetleri, perakendeciler ve kamu kurumları, çoğu olayın sorumlusu kötü niyetli suçlular tarafından en fazla ihlali yaşamıştır. Bu sektörlerden bazıları finansal ve tıbbi veriler topladıkları için siber suçlular için daha caziptir ancak ağ kullanan tüm işletmeler müşteri verileri, kurumsal casusluk veya müşteri saldırıları için hedef haline gelebilir. Siber tehdidin ölçeği artmaya devam ederken International Data Corporation, dünya çapında siber güvenlik çözümlerine yapılan harcamaların 2022'ye kadar 133,7 milyar dolara ulaşacağını öngörüyor. Dünyanın dört bir yanındaki hükümetler, artan siber tehdide karşı bir yanıt olarak kuruluşların etkili siber güvenlik uygulamalarını yürütmelerine yardımcı olmak için onlara rehberlik etmiştir. ABD'de Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bir siber güvenlik çerçevesi oluşturmuştur. Kötü amaçlı kodun çoğalmasıyla mücadele etmek ve erken algılamaya yardımcı olmak için bu çerçeve, tüm elektronik kaynakların sürekli ve gerçek zamanlı olarak izlenmesini önerir. Sistem izlemenin önemi, Birleşik Krallık hükümetinin Ulusal Siber Güvenlik Merkezi tarafından sağlanan "10 adımda siber güvenlik" kılavuzunda vurgulanmıştır. Avustralya'da Avustralya Siber Güvenlik Merkezi (ACSC), kuruluşların en güncel siber güvenlik tehditlerine nasıl karşı koyabilecekleri konusunda düzenli aralıklarla kılavuz yayınlar. Daha detaylı bilgi için tıklayınız.

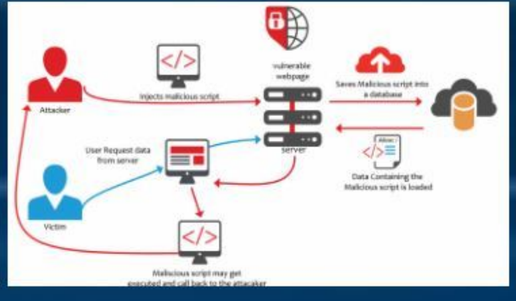
İnsanlar zaman içinde teknolojinin gelişmesi ile birlikte birçok işi daha kolay yapmaya başladılar.Üşenen insan hep daha kolay bir yol arar bu herzaman kötü bir şey degildir bulunan pek çok icadın temeli bundan kaynaklıdır.Aynı şekilde bankacılık, yiyecek, içecek, giyim ve birçok alanda artık tek tıkla işlemlerimizi halledebiliyoruz.Peki bunları yaparken ne kadar güvendeyiz hiç düşünüz mü ? Teknolojinin gelişmesiyle beraber ***siyah şapkalı hackerlar*** diye tabir ettiğimiz buldukları kod açıklarını sömürmeye çalışan ve bu açıklar sayesinde insanlara maddi manevi zarar veren kişilerin sayısı gün geçtikçe artmaktadır. Tabi ki her kötünün karşısında bir iyi olmalı ki düzen sağlanabilsin.İnterneti güvenli bir yere getirmeye çalışan hackerlara ***Beyaz şapkalı hackerlar*** denir. Beyaz şapkalılar güvenlik zaafiyetlerini düzeltmeye çalışırlar ve bunun için denetim yapacağı firmalardan onay almak zorundadırlar. Tabi ki bilindiği kadarıyla bunlar geçerlidir. Yin Yang felsefesine göre her siyahın içinde beyaz bulunduğu gibi beyazın içinde de siyah bulunmaktadır. Ama genel itibariyle bakarsak beyaz şapkalılar bizim dostlarımızdır. Bunun yanında ***Gri şapkalı hackerlar*** dediğimiz bir grup bulunur. Bunlar ise izinsiz bir şekilde sisteme sızıp açıkları düzeltirler veya bildirirler.

İnternette korunmak için bir şeyleri sadece Beyaz Şapkalılardan beklememeliyiz. İnternette korunmak için bilmediğimiz websitelerine, tanımadığımız kişilerden gelen linklere, davetlere tıklamamalıyız. Eğer gerekirse Browserlarımızın güvenlik kısmından gerekli ayarları yapıp browserda script çalışmasını engellemeliyiz.

İnternette korunmak için bir şeyleri sadece Beyaz Şapkalılardan beklememeliyiz. İnternette korunmak için bilmediğimiz websitelerine, tanımadığımız kişilerden gelen linklere, davetlere tıklamamalıyız. Eğer gerekirse Browserlarımızın güvenlik kısmından gerekli ayarları yapıp browserda script çalışmasını engellemeliyiz.

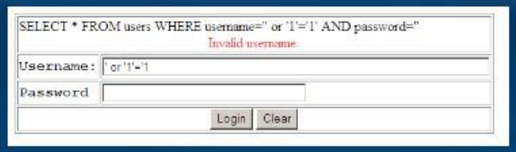
XSS

XSS script kodları üzerinden bir web sayfasına saldırı yapılmasıdır. Bunun Reflected ve Stored olmak üzere 2 çeşit tipi vardır. Stored adından anlaşılacağı gibi siteye depolanmış bir script vardır. Bu siteye giren herhangi biri browser ayarlarından script çalıştırma seçeneğini seçmez ise hacker o ziyaretçi üzerinde türlü script dosyaları çalıştırabilir. Reflected ise genelde pshing saldırılarıyla birleştirilerek kullanılır. Enjekte edilen kodun urlsi alınır ve türlü pshing saldırılarıyla genellikle kısaltılmış link olarak hedef kişiye gönderilir.



SQL Injection

SQL Injection, veri tabanına dayalı uygulamalara saldırmak için kullanılan bir atak tekniğidir; burada saldırgan SQL dili özelliklerinden faydalanarak standart uygulama ekranındaki ilgili alana yeni SQL ifadelerini ekler. (Örneğin saldırgan, veritabanı içeriğini kendisine aktarabilir).[1] SQL Injection, uygulamaların yazılımları içindeki bir güvenlik açığından faydalanır, örneğin, uygulamanın kullanıcı giriş bilgileri beklediği kısma SQL ifadeleri gömülür, eğer gelen verinin içeriği uygulama içerisinde filtrelenmiyorsa veya hatalı şekilde filtreleniyorsa, uygulamanın, içine gömülmüş olan kodla beraber hiçbir hata vermeden çalıştığı görülür. SQL Injection, çoğunlukla web siteleri için kullanılan bir saldırı türü olarak bilinse de SQL veri tabanına dayalı tüm uygulamalarda gerçeklenebilir. SQL injection saldırıları, saldırganların, sistemdeki kullanıcılardan birinin bilgileriyle giriş yapmasına, mevcut verilere müdahale etmesine, bazı işlemleri iptal etmesine veya değiştirmesine, veri tabanındaki tüm verileri ifşa etmesine, veri tabanındaki tüm verileri yok etmesine, veri tabanı sunucusunda sistem yöneticisi olmasına olanak sağlar.



BruteForce

BruteForce diger adıyla Kaba kuvvet saldırısı bütün kombinasyonları deneyerek şifre kıran saldırı türüdür. Bu saldırı türü gerçekten sabır işidir. Bunun için zamanla özel wordlistler hazırlanmaya başladı ve kişinin sevdiği, değer verdiği, evcil hayvanı gibi şeyleri pasif aramayla öğrenip özel wordlistler hazırlanır bunlara örnek bir tool verirsek cupp'tur. Alternatif olarak kali linux gibi çekirdeklerte rockyou.txt, fasttrack.txt gibi wordlistler kullanabilir veya internetten özel olarak birkaç wordlist bulabilirsiniz. Bu wordlist saldırılarından korunmanın en iyi yolu uzun ve komplike bir şifre koymaktır. Bunun için sembol, sayı, büyük ve küçük harfler kullanmalıyız. Unutulmamalıdır ki kırılamayacak şifre yoktur. Fakat önerdiğim şekilde bir şifre koyarsanız muhtemelen değil hackerin torunlarının bile ömrü yetmeyecektir.

TROJEN

Truva atı, Odysseus'un (Akhalılar) Truva surlarını aşmak ve şehre (Troya'ya) gizlice girmek için yaptırdığı tahtadan at maketidir. Savaş yaklaşık 10 yıldır sürmüştür. Askerler bıkkın ve yorgundur. Zekası yüzünden Athena tarafından da sevilen Odysseus'un aklına tahtadan bir at yapma fikri gelir. Plana göre Akhalılar savaştan çekiliyor gibi gözüküp, geride çok büyük bir tahta at bırakırlar. Odysseus ve diğer seçkin komutanlar atın içine gizlenirken, diğerleri denize açılıp gemileri Bozcaada'nın arkasına, Troyalıların onları göremeyeceği bir şekilde gizlerler. Planın yürümesi için, görevi tahta atın Truvanın surlarından içeri girmesini sağlamak olan bir Akhalı askeri atın yanında bırakırlar. Akhalıların çekildiğini gören Truvalılar, şaşkınlık içinde batı kapısının önündeki dev tahta atın yanına giderler. Bu sırada ortaya çıkan Sinon ismindeki Akhalı asker, Yunanlardan nefret ettiğini, onu Akhalıların geri dönüşleri için gerekli rüzgarın çıkması adına kurban seçtiklerini ve kendisinin kaçarak kurtulduğunu söyler ve şöyle devam eder: Tahta at Tanrıça Athena'ya kutsal bir sunak olarak yapılmıştır. Büyük olmasının sebebi Troyalıların onu dar şehir kapılarından şehrin içine almalarını engellemek içindir. Akhaların beklentisi Troyalıların bu atı yakıp yıkmalarıdır. Böylece Tanrıça Athena'nın öfkesini Troya üzerine çekmiş olacaklardır. Ama Troyalılar atı şehrin içine alıp onu korurlarsa Athena'nın lütfu Troyalılara yönelecektir. Ahkalı askerin sözlerine inanan barışmak isteyen Truvalılar bu sözlere inanırlar ve tahta atı içeri alırlar. Gece barış kutlamalarıyla eğlenen ve alkolün etkisiyle sızan Truvalılar, atın içindeki Akhalı Savaşçılar tarafından avlanır. Bu sırada Truva'nın surlarına yaklaşmış olan Akhalı Ordusunun da takviyesiyle Truva Şehri tamamen yıkılır.
Trojen ise bu mantıkla çalışır bir dosyanın içine virüs yerleştirilerek çeşitli sosyal mühendislik yöntemleriyle karşı tarafa yutturulmaya çalışılır. Eğer kişi bunu anlamayıp indirdiyse ve çalıştırdıysa karşı tarafa bir session açtırmış olur. Hacker bu saatten sonra bilgisayarınızdaki olan bütük olayları izleyebilir, yönetebilir, bilgi çalabilir çeşitli programlar, çalıştırtabilir veya indirtebilir. Ayrıca bu videoyu eğlenmeniz ve bilgi edinmeniz için tavsiye ederim. Fakat intro kısmında sesi kısmayı unutmayın.

RANSOMWARE

Ransomware saldırıları çok tehlikelidir. Eğer bir şekilde script kodu çalıştırabilir veya bir şeyler indirtebilirlerse size bütün dosyalarınızı şifreleyip size para karşılığı geri vereceklerini söylerler. Fakat gerçekten verirler mi bu bir bilinmezliktir. Bana göre yiyebileceğiniz en kötü saldırı budur. Bu tarz saldılarının bazılarının çözümü vardır bazılarının ise kesin bir çözümü yoktur. Verilerinizi belirli aralıklarla depolamanızı öneririm.

PHISHING SALDIRISI

Phishing, internet tarihinin en eski ve en etkili saldırı türlerinden biridir. Oltalama saldırıları olarak bilinen bu saldırı türünde genel olarak kurbanların e-posta hesaplarına; hediye, indirim, veya benzeri cezbedici sahte iletiler gönderilerek parola, kimlik bilgisi veyahut benzeri hassas verilerin çalınması amaçlanır. İletilen e-posta mesajlarındaki zararlı bağlantılar tıklandığı zaman kurbanın av olması sağlanabildiği gibi e-postalar ile birlikte ek olarak gönderilen virüslü dosyaların çalıştırılması ile de kurbanların bilgisayarları saldırganlar tarafından ele geçirilebilir. Bankanızın, e-postanızın, sosyal medya hesabınızın veya bunun gibi bilgi girmenizi gerektiren bir kuruluşun web sayfasının bir kopyasını oluşturarak kullanıcının hesap bilgilerini çalmayı hedefleyen bir İnternet dolandırıcılığı türüdür. Bu yöntem ile dolandırıcılar sizin kredi kartı, banka giriş bilgileri, şifreler, hesap numaraları, sosyal medya hesap bilgileri gibi sizin için önemli olan bilgileri ele geçirmeyi hedefliyorlar.Devamı İçin Tıklayın

Evil Twin

Evil Twin Saldırıları hedeflenen ağdan bir ağ klonlar ve hedeflemiş olduğu ağı deauthentication(yetkisizlendirme) saldırısı yaparak erişimenizi imkansız hale getirir. Böyle klonlanan ve aynı isimde olan ağa baglanmanız beklenir. Modem de güncelleme var veya farklı bir sosyal mühendislikle kandırıp wi-fi şifrenizi çalmayı hedefler.

Contact Form

Name

Name

E-mail

E-mail

Telephone number

+905*********

Submit