EXPLOIT

Alt Başlık

EXPLOİT

- **EXPLOİT** Türkçeye “Sömürme” veya “Yararlanma” olarak çevrilebilir.
- Sisteme sızarak yetkisiz kullanıcı profiline yönetsel yetkilerin kazandırılması ve sömürme işlevine “Exploiting” denir. Yetki yükseltme işlemlerinin kullanıldığı uygulamalara ise “Exploit” denir.

EXPLOİT

- Exploit bir kötücül yazılım değildir, daha çok bir metottur. Siber suçlular tarafından hazırlanan bir program veya bir kod parçacığıdır. Bu program veya kod parçacığı hedef sistemde var olan bir açıklık kullanılarak sisteme iletilir ve sisteme sızılmaya çalışılır. Sisteme sızıldıktan sonra sistemde hedeflenen amaçları gerçekleştirmek için yetki yükseltilerek, kullanıcı profilinden yönetici profiline geçilir. Bu işleme Exploiting denir.

BİR EXPLOIT NASIL ÇALIŞIR?

- Güvenlik açıklarının çoğunluğu bir yazılım veya sistem mimarisi hatasının sonucudur. Yanlış tasarım veya eksik kodlama gibi hatalar sonucunda sistemde çeşitli açıklıklar meydana gelir.
- Kötü niyetli kullanıcılar tarafından, hedeflenen sistemde var olan açıklıklar bulunur. Daha sonra bulunan açıklıklardan hedef sisteme, siber suçlular tarafından hazırlanan bir program veya kod parçacığı iletilerek sisteme ulaşılmaya çalışılır. Sisteme ulaşıldıktan sonra sistemde istenildiği gibi hareket etmek için, kullanıcı profilinden yönetici profiline geçilmeye çalışılır. Bu da yine sistemde var olan açıklıklar kullanılarak gerçekleştirilir.

AÇIKLIK NOKTALARI

- Donanım
- Yazılım
- Ağ
- Personel
- Fiziksel Site

Donanım

- Donanım, çeşitli derecelerde, ister bir kişisel bilgisayar için karmaşık işletim sistemi olsun, ister bir uç cihaz için daha basit bir işletim sistemi olsun, bir işletim sistemi üzerinde çalışmalıdır. İşletim sistemindeki güvenlik açıklıkları, belleği bozabilecek veya cihazın donmasına neden olabilecek bir istismar için giriş noktaları haline gelir.

Yazılım

- Yazılım geliştirmenin normal bir sonucu olan yazılım hataları, yama yapılmadığı veya düzeltilmediği takdirde kötüye kullanıma açık güvenlik açıkları haline gelebilir. Yaygın exploit metotlarından bazıları arasında bellek güvenliği ihlalleri, giriş doğrulama hataları, yan kanal saldırıları ve privilege confusion (ayrıcalık karışıklığı) hataları yer alır

Ağ

- Bir ağın bileşenlerinin her biri, donanım, yazılım veya güvenlik duvarı yapılandırmaları olsun, güvenlik açığı olasılığı sunar. Açıklardan yararlanmanın bir parçası olabilecek bazı saldırılar; alanın ele geçirilmesi, DoS ve dağıtılmış hizmet reddi (DDoS) saldırıları ve kötü amaçlı yazılım olabilir

Personel

- Personeller de exploit edilebilir. Siber suçlular, sosyal mühendislik saldırıları, hedef odaklı kimlik avı ve bal tuzağı yoluyla cihazlarını ve kimlik bilgilerini hedef alabilir. Eğitim ve erişim kontrolü bu güvenlik açığını azaltmak için çok önemlidir.

Fiziksel Site

- Exploiting, fiziksel güvenliğin veya yetersiz erişim kontrolünün mevcut olması durumunda site üzerinde gerçekleştirilebilir. Bir hırsızın içeri girip hırsızlık yapabilmesi gibi, bir siber suçlu da(fiziksel veya uzaktan) içeri girip tüm ağı tehlikeye atacak bir istismar gerçekleştirebilir. En yaygın web tabanlı güvenlik açıklıklarından bazıları arasında SQL enjeksiyon (injection) saldırıları, siteler arası komut dosyası oluşturma, (cross-site scripting) ve siteler arası istek sahteciliğinin (cross-site request forgery) yanı sıra bozuk kimlik doğrulama kodunun (broken authentication code)kötüye kullanılması veya güvenlik yanlış yapılandırmaları (security misconfigurations) yer alabilir[3][5].

EXPLOIT TÜRLERİ

a) Zero-Day (Bilinmeyen) Exploitler

- Bu, daha önce bilinmeyen bir exploit veya güvenlik açıklarından dolayı bilinmeyen bir exploit fırsatıdır. Bir sistemde, uygulamada tespit edilen bir açığa, çok kısa bir süreçte yazılan exploitlere Zero-Day exploit adı verilir. Zero-Day exploitler henüz ilgili sistemde, uygulamada yama çıkarılmadan yayınlandığı için tehlikeli olabilmektedirler. Zero-Day exploitleri tahmin etmek, güvenlik açığını veya tehdidi azaltmaya yönelik yamalar veya başka stratejiler geliştirmek açısından çok önemlidir

b) Bilinen Exploitler

- Bilinen exploitler tespit edilmiş ve belgelenmiş olanlardır. Yamalar ve diğer düzeltmeler yayınlanabilir, ancak siber suçlular aynı zamanda belgeleri ele geçirip bir istismar tasarlayabilirler. Ana risk faktörü, kuruluşların genellikle bir güvenlik açığını ortadan kaldıracak kadar hızlı bir şekilde yamayı uygulamamaları veya bir sorunu onarmamalarıdır[

ERİŞİM ŞEKLİNE GÖRE EXPLOITLER

a) Local Exploitler

- Genellikle sisteme (local olarak) normal kullanıcı yetkileriyle bağlanan kullanıcıların, yetkilerini yükseltmek amacıyla, sistemde bulunan açıkları sömürmek için kullandıkları exploitler olarak tanımlanabilir.

b) Remote Exploitler

- Remote Exploitlerde, harici bir bilgisayarda, intranet veya başka bir ağ aracılığıyla çalıştırılarak, sisteme önceden erişim gerekmeden bir güvenlik açığından yararlanılır. Amacı, verilere erişmek veya verileri çalmak ya da tek bir bilgisayara veya tüm sisteme veya ağa kötü amaçlı yazılım yüklemektir. Sisteme (Herhangi özel bir yetki olmaksızın) uzaktan bağlanan kullanıcıların, uygulama üzerindeki açıkları sömürmek için kullandıkları exploitlerdir.

EXPLOIT KİT

- Exploit kitleri, kullanıcının web’de gezinirken bilgisayarında belirlenen güvenlik açıklarından sessizce ve otomatik olarak yararlanmaya çalışır. Tarayıcı açıklarından yararlanmalar genellikle kullanılır, ancak bunlar aynı zamanda Adobe Reader gibi yaygın yazılımları veya işletim sisteminin kendisini hedef alan açıkları da içerebilir. Kitlerin çoğu PHP'de yazılmıştır. Çoğunlukla otomatiktirler ve uzaktan erişim araçlarının (Remote Access Tools (RAT)) veya toplu kötü amaçlı yazılımların siber suçlular, özellikle de bir istismardan kâr elde etmek isteyenler tarafından dağıtımı için tercih edilen yöntem haline gelmişlerdir.

EXPLOIT KİT

- Çoğu zaman amaç, cihazların kontrolünü basitleştirilmiş ve otomatikleştirilmiş bir şekilde ele geçirmektir. Saldırının başarılı olması için bir exploit kiti içerisinde bir dizi olay gerçekleşir. Bir açılış sayfasına yönlendirmeyle başlar, ardından istismarın yürütülmesi ve son olarak da yükün teslim edilmesiyle ana bilgisayarın kontrolünün ele geçirilmesi gelir. Exploit kitleri, sistemin güvenliğini değerlendirmek için sızma testinde de kullanılabilir. Exploit kitleri genellikle karaborsada hem bağımsız kitler hem de hizmet olarak satılmaktadır

BİTTİ ☺