Bilgi Güvenliği ve Kriptoloji

Hackerler, Yöntemleri ve Araçları

Hacker kimdir?

- Bilgisayarla ve internet ile biraz haşır haşır neşir olmuş herkesin kafalarında bir "hacker" tanımı vardır. Hackerler medyada genellikle yıkıcı, kötü amaçlı bilgisayar kullanıcıları olarak gösterilirler
- Hackerler bilgisayar dünyasının dahi çocuklarıdır. Bilgisayarlar üzerinde olağanüstü bir yeteneğe ve sıra dışı bir zekaya sahip kişilerdir. Hacker genel kanının aksine sadece "bilgisayar korsanlığı" demek değildir.

Hacker kimdir?

- Hacker genel kanının aksine sadece "bilgisayar korsanlığı" demek değildir. Günümüzde kabul görmüş iki yaygın hacker tanımı var. Bunların ilki bilgisayar programcılığı, ikincisi de bilgisayar güvenliğini ele alıyor…

Hacker kimdir?

- İlk tanım ünlü hacker sözlüğü Argo Dosyası'nın (Jargon File) yazarı Eric Steven Raymond tarafından yapılmıştır. Ona göre, programlanabilir sistemler hakkında sadece gerektiği kadar bilgiyi edinmeyi tercih eden çoğu kullanıcının aksine; sistemlerin ayrıntılarını incelemekten hoşlanan ve sistem yeteneklerini geliştiren kişiye "hacker" denir.

Hacker kimdir?

- İlk tanım ünlü hacker sözlüğü Argo Dosyası'nın (Jargon File) yazarı Eric Steven Raymond tarafından yapılmıştır. Ona göre, programlanabilir sistemler hakkında sadece gerektiği kadar bilgiyi edinmeyi tercih eden çoğu kullanıcının aksine; sistemlerin ayrıntılarını incelemekten hoşlanan ve sistem yeteneklerini geliştiren kişiye "hacker" denir.

Hacker kimdir?

- Bu tanımlama hacker kavramına tamamen pozitif bir anlam yüklemektedir. Bu açıdan bakıldığında hacker'lar son derece yetenekli ve üretken programcılardır. Programcılık bakımından "hack'lemek" (hack etmek) demek, bir sistemin bilinmeyen sırlarını ortaya çıkarmak ya da sistemi belli bir amaca hizmet edecek şekilde yeniden programlamak demektir.

Hacker kimdir?

- Bu tanımlama hacker kavramına tamamen pozitif bir anlam yüklemektedir. Bu açıdan bakıldığında hacker'lar son derece yetenekli ve üretken programcılardır. Programcılık bakımından "hack'lemek" (hack etmek) demek, bir sistemin bilinmeyen sırlarını ortaya çıkarmak ya da sistemi belli bir amaca hizmet edecek şekilde yeniden programlamak demektir.

Hacker kimdir?

- Programcı hacker'lar için hacking "bir programlama problemine hızlı ve zarafetsiz olmasına rağmen işlevsel bir çözüm getirmek" demektir. Raymond'a göre bilgisayar sistemlerine zarar veren kişilere hacker değil "cracker" denir. Raymond aradaki farkı şöyle tanımlar: "Hacker'lar bir şeyler yapar, cracker'lar onları bozar…"

Hacker kimdir?

- Programcı hacker'lara örnek olarak Linux'un geliştiricisi Linus Torvalds , GNU projesinin lideri Richard Stallman ve Microsoft'un kurucusu Bill Gates gösterilebilir.
- Bu tanım ele alındığında hacker'ların pek de ilgi çekici ve gizemli kişiler olmadığı görülüyor. Ancak medyanın da etkisiyle bu klasik hacker tanımının kullanımı giderek azalmıştır.

Hacker kimdir?

- İkinci hacker tanımıysa bilgisayar güvenliği alanını kapsıyor. Bilgisayar sistemleri üstün bilgiye ve beceriye sahip, özel taktiklerle sistemlere izinsiz erişim sağlayan kişilere hacker denir. Bu tanım size daha tanıdık gelmiştir. Bizde bu tanıma uyacağız.
- Hackerler serbest bilgiye erişim özgürlüğüne inanırlar. Onların tehlikesi istedikleri bilgiyi edinmek için sisteminize saldırmalarından ve sızmalarından kaynaklanır.

Hacker kimdir?

- Hackerler için birincil amaç güvenlik sistemlerini yıkmak değildir, korunan bilgiye erişmektir.
- Hacker'lar başarılarıyla övünmeyi sevmezler. Genellikle sahne arkasında çalışırlar ve gizliliğe önem verirler.

Hacker Türleri:

- Hackerler niteliklerine ve amaçlarına göre ikiye ayrılırlar: Beyaz şapkalılar ve Siyah şapkalılar.
- Ayrıca hacker olmayan Hacker ’lığa özen gösteren kişiler için de “Lamer” ve “Script Kiddie” tanımlaması kullanılır.

Beyaz şapkalı (white hat)

- Beyaz şapkalı hacker'lar, güvenlik sistemlerini zarar vermek amacıyla kırmayan iyi niyetli hacker'lardır. Beyaz şapkalılar bir sistemin zayıf noktalarını bulmak için yazılımı üreten şirketle birlikte çalışabilirler. Beyaz şapkalılar herhangi bir sistemde tespit ettikleri açığı kamuoyuna duyurmadan önce yazılımı geliştiren firmaya/kişiye açığı bildirir, açığın kapatılması için makul bir süre tanır ve bu süre boyunca sisteme zarar vermez.
- Ardından, kamuoyunu bilgilendirmek amacıyla bu açıkla ilgili ayrıntıları çeşitli haber gruplarında ve web sitelerinde duyurur. Beyaz şapkalıların savunma amaçlı çalıştıklarını söyleyebiliriz. Bu kişilere "etik hacker" da denir.

Siyah şapkalı (black hat)

- Siyah şapkalı hackerlerde beyaz şapkalıların tam tersidir. Güvenlik sistemlerini izinsiz olarak aşarak bilgi hırsızlığı, dolandırıcılık, terörizm, bilinçli yıkım gibi zarar verici faaliyetlerde bulunurlar. Bunları bir bilgisayara uzaktan erişme ya da bir yazılımı kırma yoluyla gerçekleştirebilirler. Yazılımları kıran siyah şapkalılara "crakcer" denir.

Gri şapkalı (grey hat)

- Yasallık sınırında dolaşan hackerlerdir. Yöneticisi bulundukları yada destek sağladıkları sistemlerin zayıf noktalarını ve açıklarını tespit ederek güvenlik politikaları için yol gösterici olurlar.

Yazılım korsanı (cracker)

- Yazılımların kopyalama korumalarını kırarak izinsiz kullanılmalarını sağlayan kişilerdir. Programlama konusunda uzmandırlar, ağ güvenliği konusunda bilgi sahibi olmayabilirler.

Hacktvisit

- Toplumsal veya politik bir sorunu dile getirmek amacıyla hacking eylemlerinde bulunan kişilerdir. Amaçları kendilerine göre "kötü" veya "yanlış" olan bir şeyi duyurmak ve ilgililere bir mesaj vermektir. Unutulmamalıdır ki amaç ne olursa olsun, bir bilgisayar sistemine izinsiz erişim sağlamak suçtur ve bu tür etkinlikler desteklenmemelidir.

Lamer

- Hacking konusunda hiçbir bilgisi olmayan, öğrendiği birkaç terimle ve eline geçirdiği birkaç basit programla hava atmaya çalışan hacker özentileridir. Lamer'lar genellikle çocuk yaştaki kişilerdir ve sadece zarar vermeyi hedeflerler.

Script Kiddie

- Hacker olmamalarına rağmen en tehlikeli ve en çok korkulması gereken kişiler bunlardır. Script kiddie'ler de lamer'lar gibi hacker'lığa özenirler, fakat lamer'ların aksine bir miktar bilgi sahibidirler. Script kiddie'ler çoğunlukla sistemlere/kişilere saldırmaya, hasar vermeye ve ele geçirdikleri bilgileri kötü amaçlarla kullanmaya çalışırlar. Onlar için bir güvenlik sistemini delmek araç değil, amaçtır.

Hacker dünyasının anarşistleri olarak tanımlanabilirler

Phreaker

- Telefon ağları üzerinde çalışan, telefon sistemlerini hack'leyerek bedava görüşme yapmaya çalışan kişilerdir. Klasik phreaker'lar çeşitli elektronik devreler hazırlayarak telefon hattına özel sinyaller gönderiyordu. Telefon ağlarının modernleşmesiyle birlikte bu yöntemler gerçekliliğini yitirmekte. Modern phreaker'lar uluslararası ücretsiz hatları tespit etmek, telesekreterleri kırmak ve VoIP servislerini hack'lemekle ilgileniyorlar.

Hacking planı

- Planlı çalışmayan bir hacker'ın başarıya ulaşması çok zordur. Genel kanının aksine, hacker'lar bilgisayarlar arasında cirit atmazlar ve istedikleri sisteme her an girip çıkmazlar. Bir sistemin hack'lenebilmesi için sistematik bir çalışma gerekir. Bu çalışma, hacker'in günlerini ve hatta aylarını alabilir. Üstelik başarılı bir sonuca ulaşması da hiçbir zaman garantili değildir.

Siyah hackerlerin saldırı planı şu aşamalardan oluşur:

1. Ön bilgi edinme
2. Tarama
3. Erişim kazanma
    1. İşletim sistemi veya uygulama düzeyinde
    2. Ağ düzeyinde
    3. Servis dışı bırakma (Denial Of Service/DOS)
4. Erişimden faydalanma
    1. Program veya veri indirme
    2. Program veya veri yükleme/gönderme
    3. Sistemde/dosyalarda değişiklik yapma
5. İzleri yok etme

Siyah hackerlerin saldırı planı şu aşamalardan oluşur:

Ön Bilgi Edinme

- Bilgi edinme aşamasında, hedefe saldırı düzenlemeden önce hedef hakkında mümkün olduğunca fazla bilgi toplanmaya çalışılır. Bu aşamada şirketin alan adı (domain name) kaydı incelenir; işletim bilgileri, erişilebilen ana bilgisayarlar (host'lar),açık portlar, router'ların konumları, işletim sistemi ve sistemde çalışan servislerle ilgili ayrıntılar tespit edilir. Yani evde kimsenin olup olmadığını anlamak için kapıyı çalmaya benzer. Ciddi bir tehlike arz etmez.

Tarama

- Tarama hacker'ın ilk aşamada edindiği bilgileri kullanarak, işine daha fazla yarayacak bilgileri edinmek için ağı veya hedef sistemi taradığı bir ön saldırı aşamasıdır. Bu aşamada port tarayıcılar, dialer'lar, açık tarayıcılar vb. araçlar kullanılır ve ağ haritası çıkarılır. Sistemde faydalanılabilecek tek bir açık bile bulunduğunda hacker saldırı aşamasına geçer. Bu nedenle bu aşama risklidir ve sistemin güvenliğinden sorumlu olan kişi tarafından en kısa sürede tespit edilip engellenmelidir.

Siyah hackerlerin saldırı planı şu aşamalardan oluşur:

Erişim Kazanma

- Bu aşama asıl saldırı aşamasıdır. Hacker tespit ettiği açığa uygun exploit'i kullanarak veya yazarak sisteme sızar, LAN üzerinde veya yerel olarak, siz internetteyken veya çevrimdışıyken, aldatma veya hırsızlık şeklinde uygulanabilir. Bu aşamada oluşabilecek zarar miktarı, hedef sisteminin yapısına ve konfigürasyonuna, saldırganın becerisine ve kazanılan erişimin düzeyine göre değişebilir.

Erişimden Faydalanma

- Hacker sisteme sızmıştır ve artık kendi hükümdarlığını ilan etme vakti gelmiştir. Bu aşamada hacker sisteme zarar verebilir. Bazı hacker'lar sistemdeki diğer açıkları kapatarak ve güvenliği arttırarak farklı hacker'ların veya sistem yöneticilerinin sisteme girmesini engeller ve sistemin sadece kendilerine ait olmasını güvence altına alırlar. Hacker sisteme tekrar kolaylıkla girebilmek için arka kapı (backdoor), rootkit veya truva atı yükleyebilir. Hacker bu aşamada amacına uygun olarak sistemden dosya veya program indirerek bilgi çalabilir, dosya göndererek veya mevcut dosyalarda değişiklik yaparak sistem yapılandırmasını değiştirebilir.

İzleri Yok Etme

- Hacker sistemi kendi amaçları doğrultusunda kullandıktan sonra etkinliklerinin tespit edilmemesi için izini kaybettirmelidir. Bunun amacı sistemde daha uzun süre kalabilmek (fark edilmediği sürece önlem alınmayacaktır) kaynakları istediği zaman tekrar kullanabilmek, hacking delilerini yok etmek ve yasal sorumluluktan kurtulmaktır. İzleri yok etmek için şifreleme, ara bağlantılar kullanma (tünelleme) kayıt (log) dosyalarında değişiklik yapma gibi yöntemler kullanılır. Hacker izlerini sildiği sürece o sistemden çok uzun süre boyunca faydalanabilir veya ele geçirdiği sistemi kullanarak, o sistemle ilişkili başka bir sistem hakkında bilgi toplamaya başlayabilir.

Hackerler alet çantası

- Hackerler hedefledikleri amaçlara ulaşmak için çeşitli yardımcı yazılımlara başvururlar. Bu araçlar, yukarıda bahsettiğimiz her aşama için kullanılabilir. Hacker'ların kullandıkları araçların bazıları (örneğin bilgi toplama araçları) temelde tamamen zararsız, hatta normal bir kullanıcı için faydalı araçlar olabilirler. Bazıları ise tamamen hacking için geliştirilmiş zararlı araçlardır. Hacking araçları çoğunlukla bilgiye erişim özgürlüğüne inan kişiler tarafından geliştirildiği için ücretsiz olarak dağıtılırlar. Hatta linux tabanlı yazılımların çoğunun açık kaynaklı olduğunu görüyoruz, ancak Windows tabanlı olanlar için aynı şeyi söylemek mümkün değil. Şimdi hacker'lar tarafından kullanılan araçları kategorilere ayırarak tanıyalım.

Bilgi toplama araçları

- Bilgi toplama araçları ping, whois, traceroute gibi basit işlemleri yerine getirirler. Örneğin whois sorgusu, bir web sitesinin hangi sunucuda barındırıldığını, IP adresini, e-posta sunucusunun IP adresini ve site sahibinin iletişim bilgilerini edinmenizi sağlayabilir. Ping komutu, internetteki herhangi bir bilgisayarın size yanıt verip vermediğini anlamak için kullanılır. Normalde bir bilgisayara ping komutu gönderdiğinizde karşı taraf size bir yanıt gönderir, böylece iki bilgisayar arasındaki veri iletişim hızı hesaplanabilir. Traceroute, sizin bilgisayarınızdan giden bir verinin hedef bilgisayara ulaşana kadar hangi noktalardan geçtiğini gösterir. Bir hacker bu ara noktalardan zaafiyeti olan birine sızarak veri iletişimini kontrol altına alabilir veya veri hırsızlığı yapabilir.

Port ve Zaafiyet tarayıcılar

- Port ve zafiyet taraması yapmak, bir hacker'ın bilgi toplamak için kullanabileceği en etkili yöntemdir. Potansiyel hedef bilgisayarlarda (özellikle sunucularda) pek çok servis sürekli çalışır durumdadır. Bu servislerin dışarıdan bağlantı kabul edebilmesi için belli bazı port'ları açmaları ve dinlemede kalmaları gerekir. Varsayılan port'lar çoğunlukla değiştirilmediği için, bir hacker hangi port'un hangi program veya servis tarafından kullanıldığını kolayca anlayabilir. Hacker zafiyet tarayıcılar vasıtasıyla hedef sistemde çalışan programları/servisleri tespit ettikten sonra o program veya servisle ilgili olası açıkları ve yükseltmeleri yapılmamış ilgili açıkları araştırmaya başlayacaktır. Bulunan açıklar vasıtasıyla da sisteme erişimi gerçekleştirmesi oldukça kolay olacaktır.

Truva Atları (Trojan) / Zararlı Yazılımlar

- Truva atı efsanesini bilirsiniz. Truva kenti bir türlü savaşarak fethedilemez. Sonunda tahta bir at inşa edilir ve bu atın içi askerlerle doldurulur. At, bir hediyeymiş gibi Truvalılara sunulur ve kente girdikten sonra attan çıkan askerler Truva'nın alınmasını sağlar.
- Gelişmiş trojan'lar veya zararlı yazılımlar bilgisayar üzerinde o kadar fazla denetim imkanı sağlamaktadır ki; kullanan kişi sizin bilgisayarınızın karşısında oturuyormuş gibi onu kontrol edebilir.

Trojan kullanılarak yapılabilecek bazı şeyler şunlardır:

- Her türlü kayıtlı hesap bilgilerinizi ve şifrelerinizi çalma
- Bilgisayarınızdaki dosyalarınıza erişebilme
- Dosya indirme, değiştirme, gönderme, çalıştırma
- Yazdıklarınızı takip edebilme
- Ekranınızı görebilme
- Bağlıysa mikrofonunuzdan ve web kameranızdan ses/görüntü kaydı alabilme
- CD/DVD sürücünüzü açıp kapayabilme (bunu genelde şaka amacıyla yaparlar, eskiden (artık bu sürücüler yok ☺))
- Yazıcınıza çıktı gönderebilme
- Klavye ve fare tuşlarınızı izleme, kitleme/değiştirme
- Sizin bilgisayarınız üzerinden başkasına saldırma

Bir trojan'ı sisteme sokabilmek için genellikle hedef kişinin toplum mühendisliği yoluyla kandırılması ve ikna edilmesi gerekir. Trojan'ların hedefe ulaşabileceği yollar şunlardır:

- MSN Skype, ICQ, IRC gibi sohbet ortamları
- Sosyal Medya Araçları, Facebook, Twitter vs…
- E-posta ekleri
- Fiziksel erişim (saldırganın sizin PC'nizi kullanması)
- Web tarayıcıları ve e-posta yazılımlarındaki açıklar
- NetBIOS (dosya paylaşımı)
- Sahte programlar
- Güvensiz siteler ve yazılımlar

Trojan'lardan korunmanın en basit yolu, her şeyi «tıklamamaktır». ☺

Şifre kırıcılar (password crackers)

Yetkili bir kişinin hesap bilgilerini ele geçirmek, genellikle hacker'ın hedefine ulaşmasını kolaylaştırır. Elinde geçerli bir hesap olan hacker, exploit'lerle ya da farklı yöntemlerle uğraşmadan, doğrudan hesap bilgilerini kullanarak sisteme giriş yapabilir ve istediği bilgiyi alabilir.

Kaba kuvvet saldırısı (brute force): Mümkün olan bütün şifrelerin denenmesine ise brute force / kaba kuvvet saldırısı denir. Teorik olarak bu yöntemle her şifre kırılabilir. Ama şifre kısa olmadığı müddetçe bu yöntem pratik değildir, çünkü iyi bir şifrenin kırılması yıllar sürebilir.

Tahmin etme: Çoğu kullanıcının son derece zayıf şifreler seçtiğini öğrenmek sizi şaşırtmamalı. qwerty, 12345,0000, doğum tarihi ve gerçek isim en çok kullanılan şifrelerden birkaçıdır.

- Şifreler, kolaylıkla ele geçirilememeleri için düz metin halinde değil de kripto lanarak saklanırlar. Sifreleri (ve diğer önemli bilgileri) saklamak için çeşitli kriptografi fonksiyonları geliştirilmiştir. Bir örnek verecek olursak,"7lekiust" şifresinin MD5 yöntemiyle kripto lanmış hali "061fd09716f00fed3a8866052db55a81" olup olmadığı kontrol edilir. Sonuçtan geriye doğru işlem yapılamaz, böylece bu şifrenin anında kırılması mümkün olmaz.

- Hacker bu tür şifrelenmiş şifreleri içeren bir veri tabanında ele geçirmiş olabilir ya da sadece kullanıcı adını bildiği bir web formunu kırmaya çalışıyor olabilir. Şifre kırmanın üç yolu vardır:

Sözlük saldırısı: Sözlük saldırısı, insanların zayıf şifre şeçme eğilimlerinden faydalanır. Sözlük (dictionary) ya da kelime listesi (word list) denilen dosya, şifre olabilecek binlerce hatta milyonlarca kelimenin alt alta listelenmesiyle oluşur.

Tuş kaydediciler (keylogger):

Tuş kaydediciler, yazdığınız her şeyi gizlice kaydeden programlardır. Ancak gelişmiş tuş kaydedicilerin yetenekleri bununla sınırlı değildir. Gelişmiş bir tuş kaydedici şu özelliklere sahip olabilir:

- Yazdıklarınızı kaydetme
- Girdiğiniz web sitelerini kaydetme
- Belli aralıklarla ekran görüntüsü alma
- E-postalarınızı kaydetme ve bir kopyasını anında saldırgana gönderme
- Sohbet kayıtlarınızı tutma. vs…..

Sniffer’lar

- Sniffer kelime anlamıyla “koklayıcı” demektir. Sniffer’lar ağ üzerinden akan verileri “koklayarak” takip ederler. Sniffer, bir yazılım ve ya uygun şekilde programlanmış bir firmware içeren donanım olabilir. Sniffer’lar ağ trafiğini gizlice incelerler ve bu sırada kesinlikle trafiğe müdahale etmez ya da değişiklik yapmazlar, bu nedenle tespit edilmeleri çok zordur. Peki, bir sniffer’la ne gibi veriler elde edilebilir? Windows dosya paylaşımı, telnet,POP3,HTTP,FTP gibi protokoller son derece popüler olmalarına rağmen yapıları çok basit ve güvensizdir. Bu protokollerde kullandığınız bütün şifreler düz metin halinde sunucuya gönderilir. İşte bu tür bir sunucuya bağlanırken kullandığınız hesap bilgileri bir sniffer’la kolaylıkla yakalanabilir.

Kaynaklar

http://en.wikipedia.org/wiki/Computer_crime

http://en.wikipedia.org/wiki/Hacker_(computer_security)

Cybercrime: Security and Surveillance in the Information Age, by Brian D. Loader (Editor), Douglas Thomas

The Art of Deception: Controlling the Human Element of Security by Kevin D. Mitnick, William L. Simon

BİTTİ ☺