**Özet**

Günlük hayatımızda kullandığımız Cep Telefonlarından Tablet, TV, vb tüm cihazları internete bağlayıp internet üzerinden işlemler yapmaktayız. Peki biz bu cihazları kullanırken karşımıza çıkan her işlem için “acaba bizim bilgilerimiz çalındı mı?” şeklinde aklınızdan sorular geçiriyor olabilirsiniz. Bu makalemde sizleri bilgi hırsızlığı yapmak, kendisine bir menfaat sağlamak isteyen Hackerların (Siber Saldırganların) başvurduğu yöntemleri anlatmaya, bu gibi durumlardan kaçınmak için başvurulması gereken yöntemler nelerdir onlardan bahsedeceğim.

1. **TEMEL TERMİNOLOJİ**

Hacker kelimesi İngilizce kökenli bir kelime olup Hack kelimesinden türetilmiştir. Hack kelimesi İngilizcede “kırmak” anlamına gelmektedir. Hack kelimesi genel anlam itibari ile izinsiz erişim elde etmek anlamına gelmektedir.

Bu Hack işlemini yapan kişi içinde “Hacker” ifadesi kullanılmıştır. Hacker kelimesini Türkçe’ye çevirdiğimizde “Bilgisayar Korsanı” olarak tanımlanmaktadır. Hacker’lar ne iş yapar diye hiç haberi olmayan kişiler kendi kendine soruyor olabilir. Bu kişiler gözlerine kestirdikleri sistemleri menfaati yada keyfi olarak zarar vermek isterler.

Hackerları 3 ana başlık altında toplayabiliriz.

· Siyah Şapkalı Hacker

· Gri Şapkalı Hacker

· Beyaz Şapkalı Hacker

Bunların 3’ü de genel itibari ile tüm saldırı yöntemlerini bilirler. Fakat “Şapka” ifadesi ile belirtilen renk seçeneği onların bu bilgileri iyi yöndemi yosa kötü yöndemi kullandıklaını ifade etmektedir. Şimdi bu hackerların kullandıkları saldırı tekniklerini inceleyelim.

1. **KEŞİF AŞAMASI**

Hackerlar tarafından kullanılan teknikler aracığılı ile saldırıya maruz kalan kişi çok büyük maduriyetler yaşayabilir. Peki bunlar isbat edilemezmi diye aklınıza sorular gelecektir. Maalesef bazılarını hackerların kullandığı yöntem sebebi ile tesbit edilmesi imkansızlaşmaktadır.

Genel itibari ile hackerlar hangi teknikleri kullanmaktadır. Detaylı olarak bakalım hep birlikte;

Hackerlar öncelikle sızcakları sistemleri gözlemlemek adına izlemeye alırlar. Bunu bir network yada bir güvenlik cihazında bir sorunu çözmek gibi düşünebilirsiniz. Bunun adına trafiği dinlemek denilmektedir. İngilizce de snif diye isimlendirilmektedir.Bu işlemleri yapabilmesi için bazı araçlar bulunmaktadır. Bu tür toolları eğer bilgisayarınıza kurarsanız o toollar aracılığı ile o bilgisayarın üzerinden hangi web sitelerine gidilmiş, o web sitelerinde bir kullanıcı adı ve şifresi kullanılmış ise onların hepsini görebileceksinizdir. Bu işlem hackerlar tarafından bu işlemler sızmak istediği bu sistemler özelinde detaylı olarak yapılmaktadır. Ağ izleme yöntemi Pasif ve Aktif olmak üzere 2 şekilde yapılmaktadır.

2.1. Pasif Tarama Teknikleri

Ev ortamlarında kullandığımız yada küçük iş yerlerinde kullanılan altyapılar için bu örneklem verilebilir. Bu tür yapılarda genellikle basit network cihazı olan HUB kullanılır. Hub cihazları bildiğiniz üzere kendisine bağlı olan tüm cihazlara broadcast yayın yaparak veri alışverişi sağlamaktadır. Bunu yaparken veriyi gönderen ve alan kişilerin kullandığı cihazlar, üzerindeki Ethernet kartları özelinde kullanılan CSMA/CD algoritmasını kullanarak paketin alıcısı ve göndericisi tespit edilir. Hackerlar bu algoritmayı devre dışı bırakıp bu gelen giden paketlerin arasına girerek dinleyebilirler. Aynı şekilde isterse bu paketleri silebilir, düzenleyebilir.

2.2. Aktif Tarama Teknikleri

Bunu yukarıdaki açıklamamda ilettiğim şekilde düşünebilirsiniz. Yani network cihazları üzerinde yapılan ağ izleme metoduna aktif izleme denilmektedir. Hackerlar bu tür cihazların arasındaki trafiği dinlemek için dsniff adını verdiğimiz uygulamayı kullanırlar. Bu uygulama içerisinde çalışan macof adını verdiğimiz ve program yer almaktadır. Macof denilen bu program sayesinde o network cihazının üzerinden rastgele mac adresi üretmesine başlarlar. Örneğin bu cihazı bir Switch olarak düşünelim. Switch cihazı kendi üzerinde bağlı olan clientların mac adreslerini ve komşulardan duyduğu tüm mac adreslerini üzerinden tutmaktadır. Bu switch dediğimiz network cihazı üzerinde bu şekilde binlerce rastgele mac adresi üretilmesi sebebi ile artık bir saatten sonra cihaz bu mac adreslerini adresleyememeye başlayacaktır. Bundan sonrada direkt olarak adreslemeden üzerindeki trafiği ya eritmeye çalışır yada cihazın crash(kilitlenme) olmasına sebep olacaktır.

Port Taraması: Siber saldırı yapacak hackerlar öncelikle saldıracakları sistemlerde hangi sistemler için hangi portlar açık. Kritik sızabilecekleri bir port varmı şeklinde bakmaarı gerekiyor. Bunun için sistemi komple öncelikler açık olan portlarını çıkartır. Bu işleme port taraması denilmektedir.

Ping Taraması:Karşı tarafa doğru ICMP portları ile bir tarama gerçeklştirilmesi ve cevap verip vermediği şeklinde kontroller yapılabilir.

Connect Scan: Bu en güvenilir tarama türüdür. Fakat yapılan bağlantılarda hemen farkedilmesi muhtemel yöntemdir. Bundan dolayı hackerlar tarafından iz bırakma konusunda ince detaylarla ilerleyen kişilerin genellikle tercih etmediği yöntemlerdir.

SYN Scan: Bu tarama türü oldukça gizlidir. Hedef alınan sistemlere SYN bayraklı paket gönderilerek yapılır. Bunun karşılığında hedef makina o portlar açık ise SYN+ACK cevabı döner Kapalı ise RST+ACK paketleri dönecektir. Bu taramayı nmap -sS -v [Hedef\_Alınan\_IP] olarak yapılmaktadır.

FIN Scan: Bu tarama türü TCP isteği yapılmadan kullanılan bir tarama yöntemidir. Eğer ilgili portlar açık değil ise RST+ACT cevabı dönecektir. Bunu yine nmap -sF -v [Hedef\_Alınan\_IP] komutu ile yapmaktayız.

Vulnerability Assessment (Zafiyet Taraması): Güvenlik açıklarının bulunabilmesi için otomatik toollar aracılığı ile yapılan otomatik kontroller diyebiliriz. Bunlardan etkin bir şekilde kullaılan zafiyet tarama tool olarak NESSUS uygulamasını söyleyebiliriz.

Enumeration (Numaralandırma): Hackerlar hedef aldıkları sistemleri öncelikle taramak için nerelere odaklanması gerektiğini anlaması ve onu belirlemesi açısından bu işlemi yaparlar. Tüm ağın üzerinde yetkisiz erişimle erişebileceği unutulmuş bir dosya paylaşılmış bir veri vs varmı şeklinde kontrol gerçeklştiriler. Bunları otomatik yapan yine toollar bulunmaktadır. Bunlardan başlıcaları Sid2User, Cheops (Linux only), UserInfo, UserDump, DumpSec, Netcat, NBTDump uygulamaları güzel örneklerdendir.

1. **GERÇEK SALDIRILAR**

Hackerların bu konuda yaptığı birçok saldırı türü bulunmaktadır. Fakat bunlardan ençok kullanılan yöntemleri birlikte inceleyelim.

3.1. SQL Injection

SQLinjection veri tabanlarına dayalı uygulamalar için kullanılan saldırı yöntemlerindir. Bunun sebebi genellikle yanlış kod yazımlarından kaynaklı yada veriyi göstermemesi gereken noktalarda gösterdiği için oluşur. Bunun önlenmesi adına firmalara güvenlik kod yazılımı ile ilgili eğitimler verilmesi ve bu metodlar hakkında hepsinin bilgilendirilmesi gerekmektedir. Çünkü hackerlar bir yazılımcıdır. Yazılımı iyi bildikleri gibi aynı zamanda sistem tarafınıda gayet hakim kişilerdir. SQL injection atak tekniği ile SQL dili özelliklerinden, standartlarından faydalanarak kafamızda bir seneryo gerçekleştirelim; Örneğin bir sayfa için giriş formu ekranı düşünelim. Bu sayfadaki veriler o sayfanın Database üzerinde tutulur sayfaya login olmak isteyen bir kullanıcı bilgilerini girmesinin ardından, o internet sayfası arkaplanda DB ye giderek sorgu çeker ve o kullanıcı adının doğru olup olmadığını teyit eder. Bu sorgu kısmında o sayfayı yazan yazılımcı arkadaş eğer SQL İnjection kontrolü yapmadan yazdı ise ozaman saldırgan SQL Sorgusunun içerisindeki koda ' OR '1'='1 şeklinde bir ekleme yaparak kullanıcı adı ve şifre ekranını atlatması münkümdür. Bu en basit örneklerden biridir. Aşağıda sorgu belirtilmiştir.

select \* from users where username='”uname'OR'1'='1”' and pass='”pass'OR'1'='1”'

3.2. XSS Zafiyeti (Cross-Site Scripting)

XSS Kemlime anlamı olarak Cross-Site Scripting anlamına gelmektedir. Yüzeysel olarak ifade edecek olursakveri giriş yapılan bir sayfada, veri girişi yapılan bu alanlar kullanılarak uzaktan kod çalıştırma diyebiliriz. Gelin bunu bir örnek ile açıklamaya çalışalım; Örneğin eliminde bir üzerinde veri giriş yapılması beklenen bir web sitesi ekranı olsun. Bu ekranda verilerin girildiği alanda genellikle Ad, Soyad şeklinde ifadeler yazılıdır ve bu ifadeler siz o alana isminizi girdiğinizde otomatik olarak silinir. Bu alana siz birşeyler yazdığınızda eğer o yazılar gitmiyorsa bu yazılar o sayfanın kaynak kodunda yer alıyor ve XSS zafiyetine zemin hazırlamış oluyor. Bunu örneklendirecek olursak; bu alanda eğer verilen silinmez ise biz Cookie bilgilerini JAVAScript dili ile okuyabiliyoruz. Bu bilgileri girdiğimiz ekranda da bu bilgilerin okunabileceğini anlamış oluruz. Bu sayade de JAVAScript ile bu oturum bilgilerini çalabilir diyebiliriz.

3.3. Şifre Kırma

Şifre Kırma yöntemleri için bir çok yöntem bulunmaktadır. Bunlardan bazılarını aşağıda sıralamaya çalıştım.

· Windows XP/2000/NT Şifre Kırma:Win NT,XP ve 2000 aynı platform altyapısına sahiptir. Windows NT sisteminde şifrelerin hashlenmiş halleri SAM adında bir güvenlik veritabanında tutulmaktadır. SAM veritabanı dediğimiz dosyada bulunan verilerin bir kopyasıda windows’un altındaki repair klasöründe yer almaktadır.

Kullanıcılar bilgisayarında şifre girdiği esnada NT Hash ve LanMan Hash adı verilen 2 sistem tetiklenir. Şifreler öncelikle Unicode yapısına ardından da MD4 algoritmasına çevrilir. Burada devreye LanMan Hash devreye girer ve bu şifreleri hesaplamak için öncelikle toplam 14 karakter olacak şekilde bir boşluk ekler. Daha sonra bunu büyük harf olarak dönüştürür. Ardından 7 karakterlik iki kısıma böler. Her böldüğü kısım içinde zayıf bir algoritması olan DES yöntemini kullanır ve bu sayede 16 byte değerinde tek yönlü hash değeri elde etmiş olur.

Microsoft sistemlerinde kullanılan LanMan mekanizması bu sistemin en büyük açığı olarakta ifade edilebilir. Çünkü bu sistemde zayıf bir algoritma yapısı vardır. Bundan dolayı kolaylıkla kırılabilmektedir. Bunu bir örnekle açıklamaya çalışalım;

Örneğin elimizde 10 karakterli 12345abcde şeklinde bir şifremiz olsun. Buna LanMan uyguladığımızda şifre 12345ABCDE şeklini alacaktır. Ardından bunu 14 karaktere tamamlayarak boşluklar sonuna bırakılır. Şifremiz artık “12345ABCDE ” şekilde olacaktır. Bunu 2 eşit kısma bölerek şifre formatlarının “12345AB” ve “CDE ”şeklinde olmasını sağlar. Bu oluşan her bir kısım için 8byte DES algoritması kullanılır. Ardından bu çıkacak sonuçlardan elde edilen hash bilgileri L0phtcrack uygulaması ile ayrı ayrı kırılmaya çalışılır. Şifreniz eğer bu şekilde karmaşık bir şifre değil ise 1 günde bu kişi sizin şifrenizi kırabilir. Bu şifre üzerinden tüm sistemlerinize erişim sağlayabilecektir.

· SAM Dosyasını Kırmak: SAM dosyası Windows sistemlerinin devamlı olarak çökme sorunları yaşaması gibi durumların önüne geçmek için kullandığı yedekleme için kullanılan bir sistemdir. Sam dosyasını ulaşılması durumunda bilgisayar üzerinde daha önceden giriş yapılmış olan şifrelerin hash bilgilerine ulaşılabilmektedir. Bunları sonrasında çeşitli uygulamalar aracılığı ilede rahatlıkla ulaşılabilir. Örneğin ophcrack uygulaması bunlar için ilk sırada gelen uygulamalardan bir tanesidir.

3.4. Kötü Amaçlı Yazılım Oluşturma

Kötü amaçlı yazılım oluşturmak için bir sürü tool bulunmaktadır. Bu toollardan birtane örnek vermeye çalışalım.

· TeraBIT Virus Maker: Oldukça zararlı bazı kötü amaçlı yazılımlar oluşturabileceğiniz bir uygulamadı. Bunun, bir kötü amaçlı yazılım oluşturucunun sahip olduğu tek seçenek olmadığının farkında olmak önemlidir. İnternette virüs oluşturmaya yardımcı olan bir dizi araç vardır. Fidye yazılımı geliştirme kitleri bile var.

3.5. Windows Hacking Teknikleri

Windows işletim sistemlerinin haclemek adına birçok yöntem bulunmaktadır. Bunlardan birkacını aşağıdaki belirttiğim bağlıklarda birlikte inceleyelim.

· Pass the Hash Saldırısı: Windows işletim sistemlerinde AD yapısı bulunan bir şirket için bu örneği verebiliriz. Burada kullanıcılar kendi bilgisayarlarını açmak istediklerinde sunuya bir kullanıcı adı ve şifre doğrulama bilgisi göndermektedir. Bu sayede bilgisayarlarını açabilmektedirler. Hackerlar bu tarz işlemlerde bu kullanıcı bilgilerini ele geçirerek sunucu üzerinde de gerekli hakimiyeti kurabilirler. Bunun için client kendi makinasını açarken kullandığı bilgisayarın sunucu üzerinde yetkili bir hesap olmaması önemlidir. Olmadı durumunda bu tür zafiyetler çıkabilecektir.

· Net User Script: Bu tür bir saldırının yapılabilmesi için saldırganın belli başlı bazı komutlar çalıştırması gerekmektedir.

net user /domain /add localaccountname password

net group /domain "Domain Admins" /add Domain

Yukarıda belirttiğim netuser komutlarını saldırgan ele geçirdiği client makinada bir noktaya koyar. Buna istinaden bilgisayarda bir sorun olması durumunda destek için müdahale edecek admin yetkili bir arkadaş bu bilgisayarın sorunlarına bakması esnasında kendi hesabı ile login olmaya çalışacak. Bu asaşmada bu yazılan komutlar vasıtası ile kurada belirtilen normal yetkili hesabı full yetkili bir hesaba evriltecektir. Eğer bu bilgisayara bağlı olan yetkili kullanıcının hesabı full yetkili bir hesap ise saldırgan bu işlemi başarabilir. Fakat normal yetkili bir hesap ise başarısız olacaktır. Bunun için son kullanıcıya müdahale eden destek elemanlarının yetkilerinin full yetkili hesap olmaması gerekmektedir.

· Login as System: Bu saldırı yönteminden fiziksel bir müdehale gerekecektir. Burada saldırgan netwotke bağlı gözden uzakta olan bir bilgisayaraı çoğunlukla tercih etmektedir. Burada kullanın bilgisayarında kullanıcı değiştirme ekranında ekran kilitliyken erişilebilirlik butonu yer almaktadır. Bunun üzerinnden yola çıkarak saldırgan buradan birşeylere erişim sağlamaya çalışır eğer kapatıldıysa. Bunu açmak için bilgisayarını yeniden başlatarak Bootable olan linux bir işletim sistemi ile bilgisayarı açar. Ardından Windows\system32 klasöür altında bulunan magnify.exe dosyasını alıp yedekleyebilir. Bunun ismini değiştirip içerisini editleyip sonrasında tekrardan aynı şekilde isimlenidirir. Sonrasında bilgisayarı açar ve erişilebilirlik alanına erişimi açabilir. Oradan komut satırını çalıştırır ve sonrasında istediği işlemleri o komut satırı üzerinden yapabilecektir.

· Sechole:Sechole uygulamasıda yine NT altyapısına sahip işletim sistemlerinde kullanıcıların admin yetkili kullanıcı olabilmesi için kullanılan bir programdır. Bu program sayesinde NT altyapısında kullanılan Kernel32.DLL dosyasında daha önceden fark edilen bir açık aracılığı ile misafir hesap açılabilir. Bu hesap ile giriş yapılmasının ardından sechole uygulaması ile bu hesap yetkili bir hesaba dönüştürülebilmektedir

· Session Hijacking (Oturum Çalma):Session hijacking diğer adı ile oturum çalma yöntemi yukarıdaki başlılarda belirttiğim sniffing ve spoofing adımlarının bir karşımıdır. Bunun temeli bir clientın oturum açma aşamasında TCP/IP Protokolünde 3 adımdan oluşmaktadır. Bir bilgisayar hedef bir sistemde oturum açmak istediğinde öncelikle SYN ve sonrasında ISN paketleri gönderir. Bu işlemlerin ardından hedef sistemde bu gelen paketler doğrultusunda ACK denilen mesaj ile bunları onaylar. Buna el sıkışma denir.Hackerlar kırmak yada sızmak istediği sistemlerde yetkili hesaba sahip olmak ister. Bu sayede o bilgisayar üzerindeki tüm sistemlere sınırsız erişim sağlayabilir. Fakat çok güvenli olan çoğu sistemde bunu yapmak hiçte kolay değildir. Bundan dolayı yetkili birini hedef olarak seçer ve onu izlemeye alır. Bunu yaparken izlemeye aldığı yetkili kişinin kullandığı FTP,Telnet vb. güvensiz protokolleri kullanıp kullanmadığını inceler ve bunları kullanıyor ise o esnadaki ISN paketlerini duymaya çalışır bunu ele geçirmesi durumunda hacker artık o kişinin ip adresini bir DOS saldırısı yaparak yetkili kişiyi devre dışı bırakır. Hacker artık bu ip adresleri üzerinden işlem yapmaya başlar. Hacker artık daha önceden dinlemeye aldığı kişinin ISN numarasını bildiğiden dolayı yetkili kişinin oturumunu üzerinde işlem yapabilecektir. Burada tüm işlemler yetkili kullanıcının hesabı ile yapıldığı için hacker iz bırakmamış olacaktır. Tüm bu işlemlerde artık yetkili kişi görülecektir.

· Windows İşletim Sistemlerinde Delilleri Yok Etme :Windows işletim sistemlerinde tüm işlemlerin loğu event log dosyalarında tutulmaktadır. Bu dosyada olaylar 3 kategoride tutulur. Bunlar güvenlik, uygulama ve sistem dir. Bu işlemlerin hepsinde dosyalar geçici bir log dosyasında turulmaktadır. Ana kayıtlar ise \*.evt uzantılı dosyalarda tutulmaktadır. Bunlar sysevent,appevent ve secevent dosyalarıdır. Erişimi olan kullanıcılar bu dosyalara Windows>system32>config altından ulaşabilecektir. Hackerler bu loğlar için bir işlem yapmazlarsa onların loglarıda burada kayıt edilmiş olacaktır. Bunun için hackerlar genelde butür risklere girmezler ve bu sebepten dolayı NTResource Kit yazılımı üzeriden kullanılan Auditpol uygulaması ile loglamayı durdurması için bir komut gönderir. Bu sayede yapılan işlemler loglanmamış olacaktır. Ardında bu loglamanın nasıl durduğunun kayıtlarınıda elsave uygulaması ile adım adım silebilecektir. Bu sayede hiçbir işlemi loglanmamış olacaktır.

1. **PENETRASYON TESTİ**

Penetrasyon testi bir ağdaki zayıflıkları ortaya çıkartmak için yapılan hacking yöntemleri ile bunların isbat edilmesidir.

Bu işlemi çoğunlukla şirketler kendi ağıda kullandıkları sistemlerin zafiyetlerini belirlenmesi için kullanılmaktadır. Bunun için belli başlı standartlar bulunmaktadır. Gelin hep birlikte inceleyelim.

4.1. NIST 800-115

Öncelikle NIST’in tanımından başlayalım; Bilgi güvenliği yazılımları ve uygulamalarını geliştirmek ayrıca bunları kullanarak güvenlik testi yapmak için kullanılabilecek standartlar bütünü olarak nitelendirilir. NIST 800-115 ise sızma testinin genel unsurları olarak nitelendirilir. Nedir peki bu unsurlar;

· Planlama:Bu aşamada testi yapacak olan kişinin kurumdan aldığı bilgiler doğrultusunda riskli alanların nereler olabileceği çıkarılmalıdır.

· Keşif:Bu aşamada kurumun kullanmış olduğu tarayıcılar üzerinde çeşitli yöntemler kullanılarak hedef ağ ile ilgili sorunları belirlemek. Bunu yaparken manuel teknikler kullanılır.

· Saldırı:Bu aşamada testi yapacak olan kişi kurum içinde, yaptığı keşif doğrultusunda hacking tekniklerini kullanarak saldırı gerçekleştirir.

· Raporlama:Son adım olarak çıkartılan tüm bu testler sonucunda ayrıntılı bir rapor hazırlanması ve bu raporun testi isteyen yetkili kişiye teslim edilmesidir. Bu çıkartılan raporda yer alması gereken konular ayrıntılı bir şekildebelirtilmelidir. İstismar edilen bir nokta var ise nasıl istismar edildiğinin belirtilmesi ve nasıl bir işlem yapılsaydı bu açığın kapatılabileceği gibi öneriler yer almaktadır.

4.2. Ulusal Güvenlik Ajansı Bilgi Değerlendirme Metodoloji

Ulusal Güvenlik Ajansı (NSA) bilgi güvenliği için birincil sorumluluğa sahiptir. ABD hükümeti bu nedenle uygulanarak bir metodoloji formüle etmiştir. Bunu gelin birlikte inceleyelim;

· Ön Değerlendirme:

o Müşterinin beklentilerini belirleyin ve yönetin.

o Kuruluşun bilgi kritikliğini anlayın.

o Müşterinin amaçlarını ve hedeflerini belirleyin.

o Sistem sınırlarını belirleyin.

o Müşteri ile koordinasyon sağlayın.

o Belgeleri isteyin.

· Yerinde Değerlendirme:

o Açılış toplantısı düzenleyin.

o Sistem bilgilerini toplayın ve doğrulayın (görüşme, sistem gösterimi ve belge aracılığıyla gözden geçirmek).

o Değerlendirme bilgilerini analiz edin.

o İlk önerileri geliştirin.

o Sunum yapın.

· Değerlendirme Sonrası:

o Belgelerin ek incelemesini yapın.

o Ne öğrendiğinizi anlamak için yardım alın.

o Koordinasyonu sağlayın ve yazılanları rapor edin.

Yukarıda belirttiğimiz bu adımlarda gayet net ne yapılması gerektiğini açıklamaktadır. Bu aşamada sızma testinin ne olduğunun müşteriye açık bir şekilde anlatılması gerekmektedir.

4.3. PCI Penetrasyon Testi Standardı

PCI DSS bir veri güvenliği standardıdır.PCI standardı, banka ve kredi kart markadaları tarafında zorunludur. Fakat ödeme kartı endüstrisi güvenlik standartları konseyince yönetilir.

Bu standartla amaçlanan hedef kredi kartı sahtekarlığının azaltılması ve kart sahibinin üzerindeki kontrollerin arttırılmasıdır. Bu standarlar doğrultusunda dikkate edilmesi gereken spesifik noktalar aşağıdaki gibidir.

· Ön etkileşim: Bu adımda kapsam, belgeleri, katılım kuralları,başarı kriterleri ve gözden geçirme yer almaktadır.

· Gerçek sızma testi: Bu aşama hacking tekniklerinin uygulandığı kısım yer almaktadır.

· Etkileşim Sonrası: Tüm bu işlemlerin ardından son aşama olarak raporlama ve bu raporlar sonucunda çıkan düzeltme önerileri yer almaktadır.

Yukarıda belirtilen bu standartların ezberlenmesine gerek yoktur. Fakat penetrasyon testinin rastgele denemeler olmadığının bilinmesi gerekmektedir. Amac testi istenen ağdaki açıkları hackerların kullandığı yöntemler doğrultusunda ele geçirmek için gereken tüm işlemleri yapmaktır. Tüm bu işlemlerde gerçek hacking metodları uygulanmaktadır.

1. **Kaynakça**

1. Bilisim Öğretmeni URL : https://www.bilisimogretmeni.com/genel/hacker-cracker-phreaker-nedir-nasil-calisirlar.html (Erişim zamanı; Nisan, 3, 2021)

2. Travels URL: https://tr.go-travels.com/41936-how-to-recover-passwords-using-ophcrack-livecd-2626168-9868897 (Erişim zamanı; Nisan, 4, 2021)

3. Wikipedia, URL: https://tr.wikipedia.org/wiki/Hacker (Erişim zamanı; Nisan, 3, 2021).

4. Wikipedia, URL: https://tr.wikipedia.org/wiki/Nmap#:~:text=Nmap%20tarama%20t%C3%BCrleri-,TCP%20Syn%20(half%20open)%20Scan,g%C3%B6ndererek%20ba%C5%9Flatt%C4%B1%C4%9F%C4%B1%20bir%20tarama%20t%C3%BCr%C3%BCd%C3%BCr.&text=Bu%20tarama%20t%C3%BCr%C3%BCnde%20TCP%20%C3%BC%C3%A7l%C3%BC,herhangi%20bir%20%C5%9Fekilde%20iz%20b%C4%B1rakmaz. (Erişim zamanı; Nisan, 7, 2021).

5. Beyaz Net URL:https://www.beyaz.net/tr/ipucu/entry/851/sql-injection-nedir (Erişim zamanı; Nisan, 5, 2021)

6. Computer Security Fundamentals kitabi sayfa:[155-178]

7. Wikipedia URL: https://en.wikipedia.org/wiki/Payment\_Card\_Industry\_Data\_Security\_Standard (Erişim zamanı; Nisan, 10, 2021)

8. Secromix URL: https://secromix.com/blog/sizma-testi-standartlari-nelerdir/#:~:text=4.-,NIST%20SP800%2D115,unsurlar%C4%B1na%20genel%20bir%20bak%C4%B1%C5%9F%20niteli%C4%9Findedir. (Erişim zamanı; Nisan, 10, 2021)