Süleyman Demirel Üniversitesi
Fen Bilimleri Enstitüsü Dergisi

Suleyman Demirel University
Journal of Natural and Applied Science

18(1), 14-21, 2014

Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi

Tuncay YİĞİT[1], Muhammed Alparslan AKYILDIZ*[2]
[1]Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, 32200, Isparta
[2]TÜBİTAK, Kamu Sertifikasyon Merkezi, 06930, Ankara

(Alınış Tarihi: 24.12.2013, Kabul Tarihi: 18.04.2014)

Anahtar Kelimeler
Sızma testi
Bilgi güvenliği
Bilişim güvenliği
Siber güvenlik.

Özet: Bu çalışmada, sızma testlerinin önemini vurgulamak açısından, gerekli servis ve sunucu kurulumları hazırlanarak, uygun olabilecek sunucu sanallaştırma işlemleri yapılmış, gerekli ağ kurulumları gerçekleştirilmiş ve sızma testleri için bir model ağ üzerinde saldırı senaryolarının değerlendirilmesi gerçekleştirilmiştir. Geliştirilen bir model ağ prototip ile uygulama alanında gerçek hayatta karşılaşılan saldırıların uygulaması yapılarak sızma testi yapılmamış sistemlerde güvenliğin nasıl geçildiği, sistemlere nasıl sızıldığı gösterilmiş, bunun sonucunda sızma testlerinin önemi vurgulanarak, siber güvenlik bilincinin oluşturulması sağlanmıştır. Sonuç olarak, prototip üzerinde yapılan deneysel çalışmalar ile sızma testlerinin önemi, bu konuda bir farkındalık oluşturularak örnek senaryolar ile sunulmuştur.

The Evaluation of Cyber Attack Scenarios Over a Network Topology for Penetration Tests

Keywords
Penetration test (Pentest)
Information security
IT Security,
Cyber security.

Abstract: The scope of this work is to investigate the effects of baffle cut and baffle spacing on the heat transfer coefficient and pressure drop in a shell and tube heat exchanger. For this aim, analyses are made for a standard dimensioned heat exchanger with variable baffle cut and spacing. It is observed that both heat transfer coefficient and pressure drops values decrease with the increase of baffle cut and baffle spacing. This paper demonstrates successful application of Genetic Algorithm for the optimal design of shell-and-tube heat exchangers. Approximate design methods for shell-and-tube have been investigated and a generalized procedure has been developed to run the GA algorithm and to find the global minimum heat exchanger area.

1. Giriş

Bilişim güvenliği, dijital ortamda depolanan bilgilerin üçüncü şahıslar tarafından ele geçirilmesini önlemek, bilgi transferi sırasında bilginin bütünlüğünün ve yapısının bozulmadan aktarılmasını sağlamak, sistemlere yetkisiz kişilerin erişmesini engellemek, sistemin sürekli olarak erişilebilir olmasını sağlamak için verilmesi gereken uğraşların tümüdür (Resmi Gazete, 2013). 20 Haziran 2013 tarih ve 28683 tarih ve 28683 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Karar" doğrultusunda bilişim güvenliği tanımı yapılmıştır.

Bilişim Güvenliği, sadece Bilgi Teknolojilerini (IT) ilgilendiren bir konu olmaktan çıkmış, bir ülkenin sağlık, enerji, hukuk, askeri alanları gibi kritik birçok konuya etki eden bir mesele haline gelmiştir. Yapılan siber saldırılar sonucu bankalara sızılabilmekte, hastanelerin veri tabanları ele geçirilebilmekte, SCADA temelli enerji sistemleri durdurulabilmekte, haberleşme sistemlerine sızılarak casusluk yapılabilmektedir. Bu nedenle, dijital ortamda depolanan bilgilerin üçüncü şahıslar tarafından ele geçirilmesini önlemek için çeşitli önlemler alınması gerekmektedir. Baykara ve diğerleri (Baykara, Daş, and Karadoğan, 2013) yaptıkları çalışmada bu önlemleri vurgulamışlardır. Bu önlemlerden biri sızma testlerinin (Pen Test) uzman kişiler tarafından gerçekleştirilmesidir. Sızma testlerinin uygulanması bilişim sisteminde var olan açıklıkların, üçüncü şahıslar tarafından bulunmadan, Bilişim Sistemi uzmanları tarafından bertaraf edilmesi, veri ve bilgi güvenliğinin gerçekleştirilmesini sağlamaktadır (Farkhod and Feruza, 2009).

* İlgili yazar: alparslan.akyildiz@tubitak.gov.tr

Siber güvenlik ile yapılan akademik çalışmaların çoğu teorik ağırlıklı ve uygulama yönünden zayıf kalmaktadırlar. Vural ve Sağıroğlu (Vural ve Sağıroğlu, 2008) tarafından yapılan çalışmada, kurumsal bilgi güvenliğinin yüksek seviyede sağlanması konusunda literatürde yeterince kapsamlı ve güncel bir çalışmanın bulunmadığına değinerek, yapılan çalışmaların çoğunlukla ticari içerikli veya güvenilir olmayan web sitelerinde yer alan yetersiz çalışmalar olduğunu belirtmişlerdir. Sadece nasıl korunulması gerektiğine ilişkin kısa bilgilere yer verildiğini ifade ederek; kurumsal bilgi güvenliği farkındalığının arttırılması için tavsiyelerde bulunmuşlardır. Rowe ve Gallaher (Rowe ve Gallaher, 2006) tarafından yapılan çalışmada, şirketlerin siber güvenlik ihtiyacının önemli olmasına karşın, pek çoğunun bu alandaki yatırımlara diğer yatırımlara nazaran daha az önem verdiklerini ifade etmişlerdir. Hoffman (Hoffman vd., 2005) tarafından yapılan çalışmada, kritik alt yapıların gittikçe sistemleri birbirine bağlayan internet ve enformasyon sistemlerine daha bağımlı hale geldiği belirtilerek, gerçek dünyanın yeniden kuruluşunda siber güvenlikte rekabetin gittikçe yoğunlaştığı belirtilmiştir. Bu nedenle kurumların bu alanda yapısal ve finansal yatırımlarının gözden geçirilmesi gerektiğine değinilmiştir. Karaarslan ve diğerleri (Karaarslan vd., 2013), "Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması" konulu sunumlarında, erişim listelerinin belirlenmesi, kullanıcı haklarının tanımlanması, erişim güvenlik duvarı, internet şifre ve sosyal mühendislik konularında ağ güvenlik politikalarının çok detaylı şekilde oluşturularak uygulamaya konulması gereğini vurgulamışlardır.

Gerçekleştirilen bu çalışmada ise, sızma testlerinin öneminin vurgulanması açısından, bir model ağ prototip üzerinde sızma senaryoları değerlendirilmiştir. Senaryolar üzerinde yapılan sızma testlerinin önemi vurgulanarak, siber güvenlik bilincinin oluşturulmasına katkı sağlanması amaçlanmıştır. Sonuç olarak, bir model ağ prototip üzerinde yapılan deneysel çalışmalar ile sızma testlerinin önemi ve bu konuda bir farkındalık oluşturularak örnek senaryolar ile alınması gereken önlemler sunulmuştur.

Makalenin diğer bölümleri şu şekilde organize edilmiştir; 2. bölümde bilişim sistemlerinde sızma testleri ve siber saldırılar konusunda teorik bilgilere yer verilmiştir. Gerçekleştirilen çalışmaya ait bir ağ prototip üzerinde sızma testi senaryoları anlatılmış ve ayrıntılı bilgiler 3. bölümde sunulmuştur. 4. bölümde ise ve sızma testleri sonucunda bulunan açıklıklara karşı alınması gereken önlemlere yer verilmiştir.

2. Bilişim Sistemleri Üzerinde Uygulanan Sızma Testleri ve Siber Saldırılar

Makalenin bu bölümünde bilişim sistemleri üzerinde uygulanan Sızma Testleri ve Siber Saldırılar hakkında bilgiler verilmiştir.

Siber ortamda gerek bireyler gerek toplumlar gerekse de ülkeler açısından çok hayati bilgilerin yer alması, siber ortamı kötü niyetli kişi, kurum ve devletler için açık bir hedef haline getirmiştir. Ünver ve Canbay (Ünver ve Canbay, 2013), "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", konulu çalışmalarında siber saldırılarda kullanılan ; virüs, kurtçuk (worm), truva atı (trojan), zombi , yemleme (phishing) ve istem dışı elektronik posta (spam) konularına değinerek bu konularda bilgi aktarmıştır.
İster sızma testi yapacak kişi için isterse kötü niyetli bir saldırgan için sistemdeki açıklıkların bulunması, bu açıklıkların kullanılması ile sisteme sızılması aynı adımlar ile gerçekleştirilir. Buradaki tek fark kötü niyetli kişilerin sistemlere zarar vermesi yada bilgi çalması, güvenlik uzmanlarının ise açıkları kapatmasıdır. Sızma testleri yapılırken sistem bağımsız olarak uygulanması gereken adımlar vardır. Bu adımlar bilgi toplamak, keşif yapmak, zafiyetleri bulmak, zafiyetleri istismar etmek ve sistemi ele geçirmektir. Bu aşamalar sızma testlerinin yaşam döngüsünü oluşturur. Bu adımlar aşağıdaki gibi örneklendirilebilirler.

Adım 1: *Bilgi Toplama aşaması;* örneğin internet üzerinden, arama motorlarından, e-posta gruplarından, DNS ve WHOIS kayıtlarından ve GOOGLE'dan bilgi toplanması gibi,

Adım 2: *Keşif aşaması*; örneğin port taratmak, banner yakalamak, çalışan servisleri belirlemek, veri tabanları hakkında bilgi toplamak ve ağ haritalamak gibi,

Adım 3: *Zafiyet tarama aşaması*; örneğin herhangi bir zafiyet tarama aracı ile veya manuel olarak açıklıkların tespit edilmesi gibi,

Adım4: *Açıklıkların istismar edilmesi aşaması*; örneğin SQL açıklığı olan bir veri tabanı sistemine SQL kodları kullanılarak SQL injection yapılması gibi,

Adım5: *Sistemin ele geçirilmesi aşaması*; örneğin sisteme sızılarak, hakların sistem yöneticisi haklarına çıkartılması gibi,

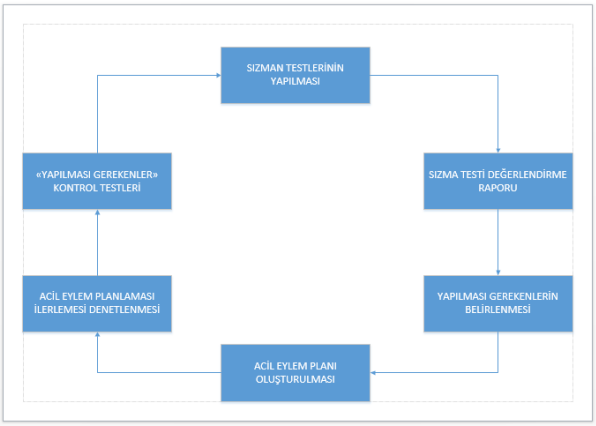
Adım6: *İzlerin temizlenmesi aşaması*; örneğin sistem günlüğü LOG'larının silinmesi,

Open Source Testing Methodolgy (OSTIMM), NIST Network Security Guide, OWASP Guide (Open Web Application Security Project), Penetration Testing Framework gibi bedava halka açık sızma testi metodolojileri sızma testi esnasında kullanılabilmektedirler. Seviyesi ne olursa olsun sızma testlerinde izlenen yol Şekil 1'de verilen sızma testi yaşam döngüsü gibi ele alınabilir. Bu yaşam döngüsü dikkate alınarak yapılan sızma testleri, güvenlik seviyesinin sürekli iyileştirilmesine katkı sağlayan ve bu yolda yapılan yatırımların ve işlerin

en az maliyetle ve en verimli şekilde yürütülmesini sağlayan bir iş modelinin temel yapıtaşıdır.

3. Uygulama Prototipi üzerinde yapılan Sızma Testi senaryoları

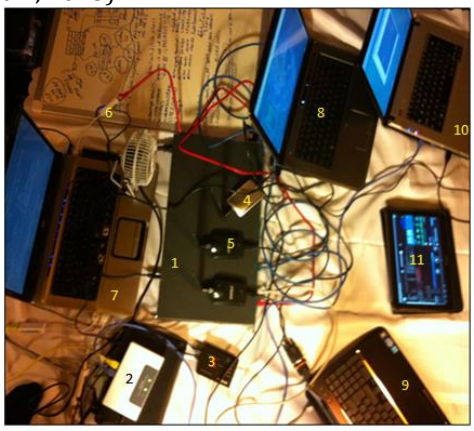
Makalenin bu bölümünde daha önceden sızma testi yapılmamış kapalı bir ağ yapısında açıklıklar test edilerek gerekli güvenlik önlemleri alınmadığı zaman oluşabilecek tehlikeler ortaya konmuştur. Ağın içerisinde bulunan erişim noktası, yönlendirici (router), switch ve çeşitli sunuculara yapılan ataklar, gerçek bir sistem üzerinde uygulanarak elde edilen sonuçlar analiz edilmiştir*.



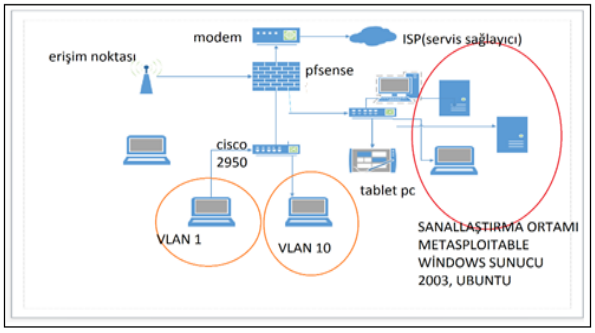
Şekil 1. Sızma testi yaşam döngüsü

3. 1. Geliştirilen uygulamaya ait bir ağ prototipi

Bu çalışmada yapılan atakların test edilebilmesi için değişik şekillerde ağ yapıları kurgulanmıştır. Ağ yapıları oluşturmak için Tablo 1'de geliştirilen uygulamaya ait ağ prototipi araç ve gereçleri etiketlenmiş ve ağ üzerindeki rolleri verilmiştir. Prototip ağ üzerinde Tablo 1'de verilen araç ve gereçlerin uygun bağlantıları yapılarak belirli saldırı senaryolarının uygulanması gerçekleştirilmiştir (Akyıldız, 2013).



Şekil 2. Uygulama ağ prototipi



Şekil 3. Uygulama ağ haritası

Saldırı senaryolarının uygulanması için Şekil 2'de uygulama ağ prototipi resmi ve Şekil 3'de de uygulama ağ haritası gösterilmiştir.

Tablo 1. Geliştirilen uygulamaya ait ağ prototipi test araç ve gereçleri

Etiket	Araç ve Gereçler	Rölü
1	Cisco layer 2 switch	Ağ içi iletişim için
2	Airties yönetilemeyen switch	Ağ içi iletişim için
3	Airties erişim noktası (access point)	Kablosuz ağ içi iletişim için
4	Alfa kablosuz ağ kartı 1 adet	Kablosuz ağ şifresi kırmak için
5	Everest kablosuz ağ kartı 2 adet	Kablosuz ağ şifresi kırmak için
6	Slink USB'den ethernete çevirici 3 adet	Güvenlik duvarı arayüzü oluşturmak
7	HP notebook 1 adet	Pfsense güvenlik duvarı yazılımı için
8	DELL notebook	Windows XP, 7, Server 2003 Metasploitable Linux işletim sistemleri ve Vmware sanallaştırma yazılımı
9	DELL notebook	Kali Linux ve Backtrack linux işletim sistemleri ile, Vmware sanallaştırma yazılımı için
10	LENOVA notebook	Backtrack linux işletim sistemi ile Dvwa, Webgoat similasyon programları için
11	SAMSUNG Tablet	Android işletim sistemi ve Son kullanıcı için

Şekil 3'deki uygulama ağ haritası incelendiğinde, uygulamaların yapılabilmesi için ağ prototipinde Pfsense üzerinde alt ara yüzler oluşturularak, üzerinde VLAN 1 ve VLAN 10 yapılandırılan Cisco switch ile Dot1q protokolü kullanılarak, switch üzerinde farklı iki ağ yapısı oluşturulmuştur. Güvenlik duvarının başka bir ara yüzüne yönetilemeyen Airties switch bağlanmıştır. Diğer ara

* Uyarı: Bu makalede yer alan hususlar ile yapılan testlerin tümü eğitim-öğretim amaçlı olup; bunların her ne şekilde olursa olsun yasadışı kullanılmasından doğabilecek sonuçlar ve yasal yükümlülükler yazarları bağlayıcı değildir. Kullanılan tüm test araçlarının, yöntemlerin, örneklerin ve yapılan testlerin yasadışı kullanılması halinde yazarlar sorumlu tutulamaz.

yüzüne ise Airties erişim noktası bağlanmıştır. Geliştirilen ağ prototipi ile internete erişim sağlayabilmesi için Pfsense güvenlik duvarı ile modem bağlantısı yapılmıştır. Ağ prototipi üzerinde mevcut bilgisayarlarda sanallaştırma ortamından yararlanılarak, Microsoft Server 2003, Metasploitable Linux, Microsoft Windows XP, Microsoft Windows 7 sanal sunucu olarak kurgulanmıştır. Sızma testi senaryolarının uygulamalarında saldırı testlerinin yapılabilmesi için Backtrack Linux ve Kali Linux işletim sistemleri kullanılmıştır. Kurgulanan işletim sistemleri üzerinde Apache Web sunucu, uzak masa üstü bağlantısı, SSH, FTP gibi servisler kurularak bu servislerden yararlanılmıştır. Ayrıca, ağlar arası iletişimin sağlanması, ve kısıtlanması gibi işlemlerin yapılabilmesi için güvenlik duvarı üzerinde paket yönlendirmesi (routing) ve paket filtrelemesi işlemleri yapılmıştır (Akyıldız, 2013).

3.2. Uygulamaya ait sızma testi senaryoları

Makalenin bu bölümünde, uygulamaya ait ağ prototipi üzerinde sızma testleri için yedi adet saldırı senaryosu verilmiştir.

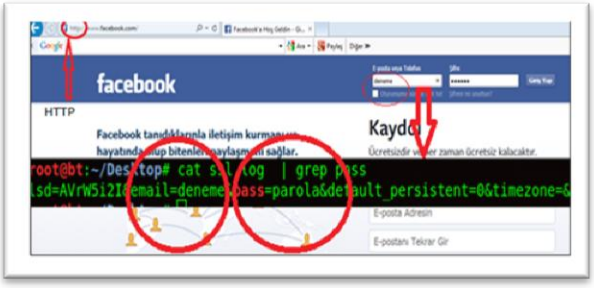
3.2.1. Senaryo I: Fiziksel uygulama testi

Fiziksel olarak cihazların yanına yaklaşılabildiği anda şifrelerin baypas edilebilmesi, gerekli güvenlik önlemleri alınmadığında atak yapan kişiler için çok basit bir hal almıştır. Fiziksel güvenliğin öneminin anlaşılabilmesi için fiziksel olarak erişilebilen bir bilgisayarın şifre baypas işlemi Şekil 4 gösterilmiştir. Windows işletim sisteminin açılışında sol alt ekranda çıkan simgenin içerisine, cmd.exe dosyasının kopyalanması ile işletim sisteminin açılışındaki şifre ekranının sol alt köşesinde bulunan ikon, utilman.exe yardımıyla terminal açılarak, admin yetkisiyle kullanıcı tanımlanabilmiştir. Daha sonra tanımlanan kullanıcı ile sisteme admin yetkisi ile giriş yapılmıştır. Bilgisayar Backtrack Linux işletim sistemi ile açılarak, cmd.exe ve utilman.exe dosyası üzerine kopyalanmıştır.

Şekil 4. Fiziksel uygulama testi

3.2.1. Senaryo II: LAN'da ortadaki adam saldırı testi

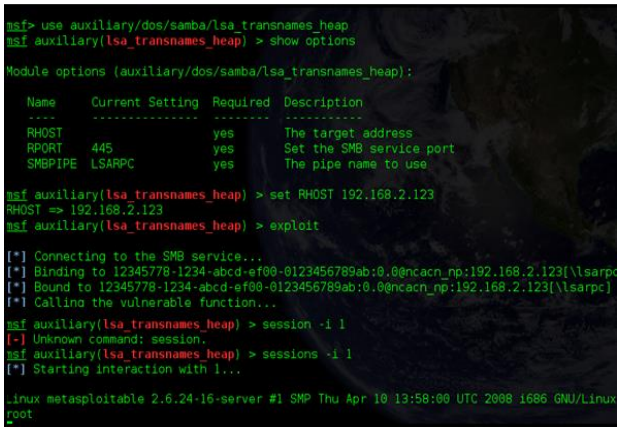
Birçok organizasyon kurum ve kuruluş dışarıdan sıkı güvenlik önlemleri almalarına rağmen, kendi iç ağ yapısında (LAN) gerekli güvenlik önlemlerini almamaktadır. Bunun sonucunda ise ağda ortadaki adam saldırıları DNS aldatmacası, STP, VTP, CDP gibi protokollerin kullanılmasıyla servis dışı bırakma saldırıları yapılabilmektedir. Ortadaki adam saldırıları ile yerel ağ trafiği dinlenilebilmekte virüs yada zararlı yazılımlar kullanılmadan, akan trafikten son kullanıcıların verileri çalınabilmektedir. SSL baypas edilerek şifreler elde edilebilmektedir. Şekil 5'de örnek bir ortadaki adam saldırısı gösterilmiştir. Ortadaki adam saldırısına uğrayan kullanıcının trafiği HTTP ile akmakta olup şifreleri Şekil 5'deki gibi alınmıştır.



Şekil 5. LAN'da ortadaki adam saldırı testi

3.2.3. Senaryo III: Sunucu tarafında yapılan saldırı testleri

Sunucular üzerinde çalışan servislerde, fuzzing gibi yöntemler kullanılarak bulunan ve istismar kodları yazılan sıfırıncı gün açıklıkları ya da (public) bilinen açıklıklar mevcut olabilmektedir. Sunucuların güncellemelerinin yapılması sıfırıncı gün açıklıklarını engelleyemese de bilinen açıklıkların kapatılması için hayati önem taşımaktadır. Şekil 6'da ise vsftpd servisi kullanan Linux işletimi sistemi buffer overflow açıklığından faydalanılarak ele geçirilmesi gösterilmiştir.

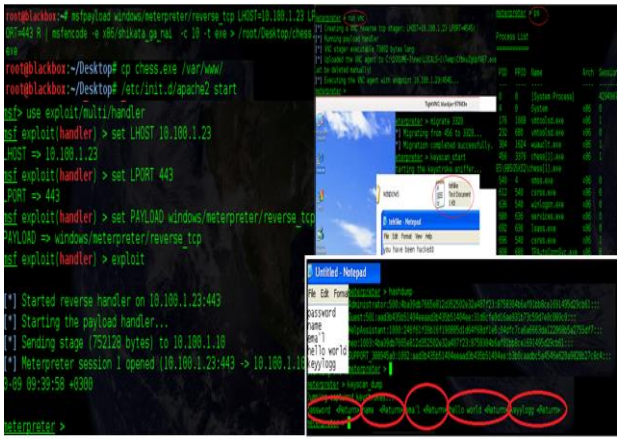


Şekil 6. Linux sunucuya sızılma test

3.2.4. Senaryo IV: Son kullanıcı tarafında yapılan saldırı testleri

Son kullanıcı (client) taraflı ataklar, son kullanıcılar tarafından kullanılan PDF, Microsoft Office, Flash, Oyun gibi uygulamaların içerisine yerleştirilen zararlı kodların, son kullanıcılara, toplu e-posta saldırıları (mass mail), yemleme (phising) ya da sosyal mühendislik yöntemleri kullanılarak gönderilmesi

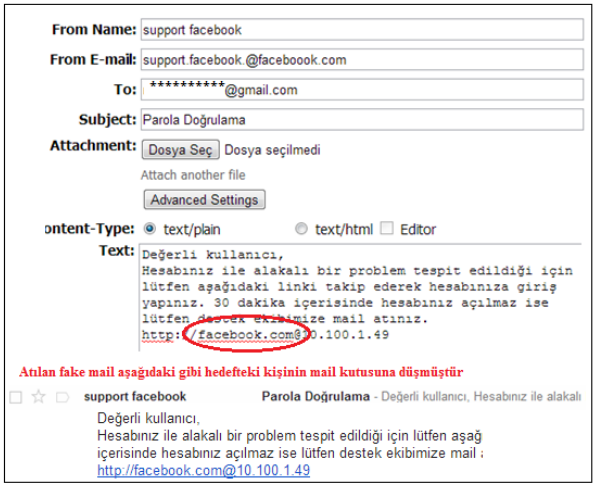
sonucunda, son kullanıcılar tarafından açılması ile bilgisayarların ele geçirilmesidir. Şekil 7'de satranç oyunu gibi oluşturulmuş zararlı kod içeren dosya son kullanıcıya gönderilmiştir. Son kullanıcının bu dosyayı açmasıyla bilgisayarının ele geçirilmesi Şekil 7'de gösterilmiştir. Son kullanıcının sistemine, yeni bir kullanıcı eklenilerek ekran görüntüsü alınabilmiştir. Ayrıca son kullanıcının bilgisayarında tuş kaydedici (keylogger) program çalıştırılarak bastığı tüm tuşlar görüntülenmiştir.



Şekil 7. Son kullanıcı (Client) tarafına sızılma testi

3.2.5. Senaryo V: Yemleme saldırıları testi

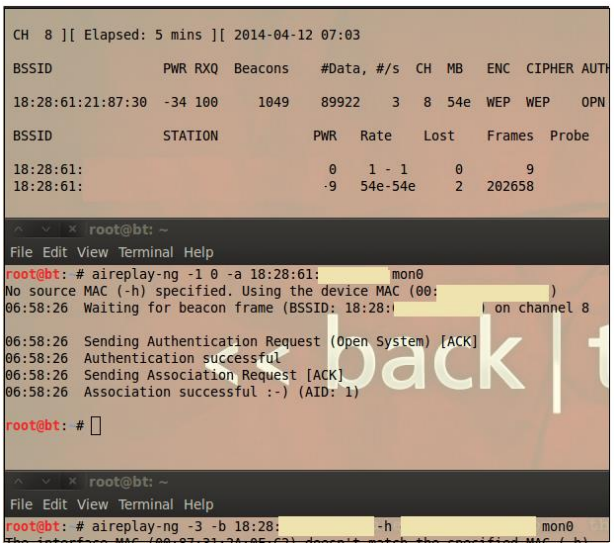
Yemleme (phising) olarak adlandırılan saldırılar sayesinde son kullanıcıların sahte sayfalara yönlendirilmesi ile şifreleri çalınabilmekte ve zararlı yazılımlar yüklenilebilmektedir. Şekil 8' de örnek bir yemleme e-posta'sı oluşturulmuştur. Bu senaryoda internet üzerinden sahte e-posta atılabilen bir siteden yararlanılmıştır. Backtrack işletim sistemindeki hazır araçlar ile yada manuel olarak yazılan programlarla da sahte e-posta atmak mümkündür. Şekil 8'de http://facebook.com@10.100.1.49 adresi facebook sitesine yönlendirmesi gerekirken adres son kullanıcıyı @ işaretinden sonraki IP adresine yönlendirecektir. Son kullanıcı linke tıkladığı anda sahte sayfaya yönlendirilecek şifreleri çalınma riskiyle karşı karşıya kalacaktır.



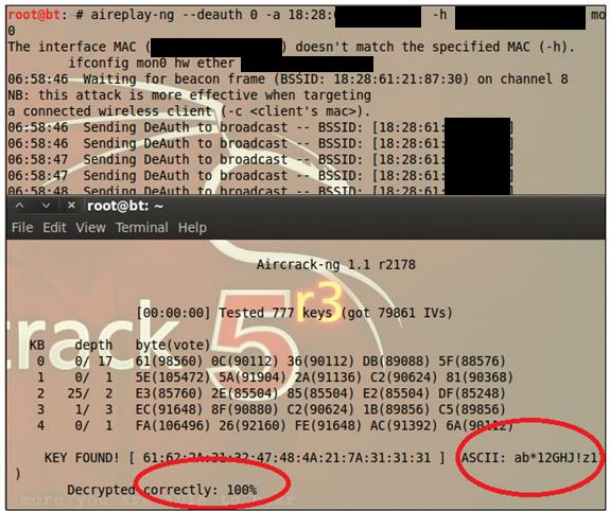
Şekil 8. Yemleme e-posta saldırı testi

3.2.6. Senaryo VI: Kablosuz ağ saldırıları testi

WEP (Wired Equivalent Privacy) şifreleme algoritması kolayca kırılabilmektedir. WPA ve WPA2 şifrelemeler ise rainbow yöntemi ile kırılabilmektedir. Kolay şifreler seçildiği zaman WPA2 şifreleri de kırılabildiği için kablosuz güvenlikte WPA yada WPA2 kullanılsa dahi şifreler karmaşık seçilmelidir. Şekil 9 ve 10'da kademeli olarak WEP şifresi kırılmıştır. Ağ kartı monitor moda alınarak havadaki tüm kablosuz yayınların görüntülenmesi sağlanmıştır. Airodump-ng aracı kullanılarak monitor edilen kablosuz ağ trafiği Şekil 9' da gösterildiği gibi yakalanmıştır. 50000 civarında yada daha fazla paket toplanarak , toplanılan paketler ile WEP şifresinin kırılması planlanlanmıştır. Burada, sahte doğrulama paketleri gönderilerek authentication 'opn' durumuna getirilir. Daha sonra arp reply paketleri enjekte edilerek toplanılan paket sayısı arttırılır. Son olarak aircrack-ng aracı ile WEP şifresi Şekil 3.10'daki gibi kırılmıştır.



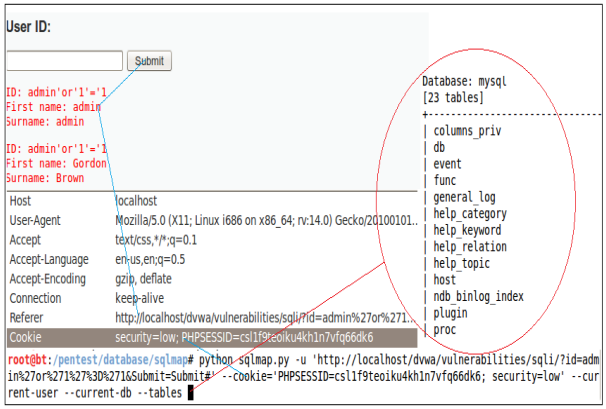
Şekil 9. Sahte doğrulama paketi



Şekil 10. WEP şifre kırma

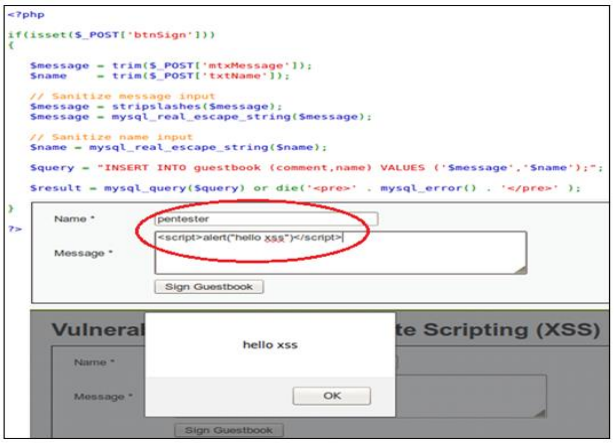
3.2.7. Senaryo VII: Uygulama alanında yapılan saldırı testi

Uygulama kodlarının çok uzun olması, insan dikkatsizliği, çalışan elemanların kalifiye olmaması gibi durumlardan dolayı uygulama tarafında string , integer , blind sql injection açıklıkları ortaya çıkabilmektedir. Örneğin SQL sorgularının filtrelenmemesinden dolayı bir sisteme ait olan veri tabanları ele geçirilebilmektedir. DWVA simülasyon programında yapılan saldırı sonucunda Şekil 11'de gösterildiği gibi veri tabanından tablolar çekilmiştir.



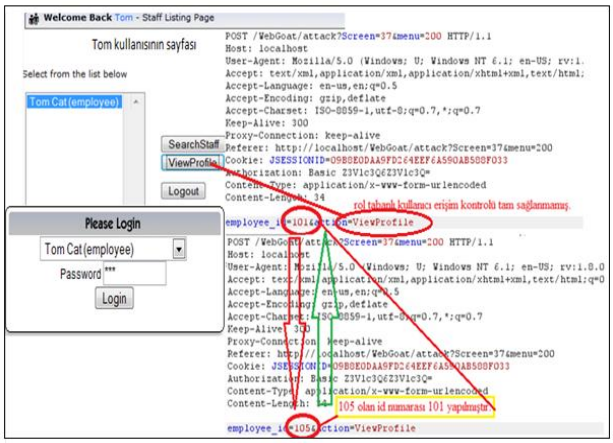
Şekil 11. SQL injection saldırı testi

Şekil 12'de kaynak kodlardan XSS açıklığı olduğu çok rahat görülebilmektedir. XSS açıklığının olduğu kutunun içerisine yazılan javascript kodları ile bu açığın olduğu gösterilmiştir.



Şekil 12. XSS açıklığı saldırı testi

Yetkilendirme hatalarından dolayı oluşabilecek bir açıklıkta Şekil 13'de gösterildiği gibi istismar edilmiştir. Burada kullanıcı kaydolurken yetki kontrolü yapılmıştır. Kullanıcı kaydolduktan sonra belirli kişilerin profillerini görüntülemeye yetkili olmasına rağmen, saldırı yapan kişi yaptığı istekleri Burp Suite aracı ile keserek kendi ID numarası ile yönetici kullanıcısının ID numarasını değiştirerek görmeye yetkili olmadığı bilgileri görüntüleyebilmiştir (Akyıldız, 2013).



Şekil 13. Yetkilendirme açıklığı saldırı testi

4. Sonuçlar ve Öneriler

Çalışmada yapılan testler sonucunda son kullanıcıların bilgisayarlarına fiziksel erişim halinde, şifreleri baypas edilmiş, ortadaki adam saldırıları ile şifreleri alınmış, sahte mailler ile farklı sitelere yönlendirilmiş, sahte e-posta atılarak truva atı saldırıları yapılmış, web sitelerindeki SQL injection, XSS açıklıkları, yetkilendirme açıklıkları gibi açıklıklar istismar edilmiş, kablosuz ağ ortamlardaki bilinen güvenlik açıklıkları incelenerek, bunların çok ciddi sonuçlara neden olabileceği görülmüştür.

Fiziksel güvenlik önlemlerinin alınması: ISO 27001 gibi standartlar göz önüne alınmalı, bu doğrultuda fiziksel olarak alanlar güvenlik seviyelerine göre ayrılmalı, izleme sistemlerinden yararlanılmalı, yetki ve sorumluluklar dahilinde giriş izinleri

tanımlanmalı, gerektiği durumlarda hard disk kriptolama yöntemleri, BIOS şifreleri, bilgisayar kilitleri ve alarm sistemleri kullanılmalıdır.

Ağ güvenliği: LAN ortadaki adam saldırısında görüldüğü üzere iç ağlarda yapılan saldırılar engellenmediğinde çok büyük güvenlik açıklıklarına sebep olabilmektedir. Yapılan uygulamada switch cihazı düzgün yapılandırılsaydı, yani arp inspection, port security, dhcp snooping, DOT1X, ipsourceguard gibi güvenlik konfigürasyonları switch üzerinde yapılmış olsaydı saldırı başarılı olmayacaktı. Öte yandan IPS, IDS, DLP, e-posta güvenlik cihazları düzgün yapılandırıldığında dışardan e-posta ile son kullanıcılara yapılan saldırıların oluşturduğu risk azaltılabilmektedir. SSL denetimi etkin hale getirilerek atak yapan kişilerin HTTPS, SSL ve TLS ile oluşturdukları tüneller engellenebilir. Burada üzerinde durulması gereken en önemli noktalardan biri ise, bir kurum yada kuruluşun cihazlara yaptıkları yatırımlardan ziyade, çalıştırdığı güvenlik personeli nitelikli değilse yapılan yatırımların boşa gittiğidir. İşe alınacak elemanların savunma (defansive) bilgi ve tecrübeleri göz önüne alınmalı, yetkin sertifikalara sahip olmalarına dikkat edilmeli, hatta ağlarda yapılması gereken güvenlikler ilgili kuruluşlar tarafından standart haline getirilmelidirler. Yukarıdaki örneklerde görüldüğü gibi switch üzerinde var olan güvenlik konfigürasyonu yapılmadığı için saldırı yapılabilmiştir. Sistemler önündeki IPS'ler açık olmadığı için sızma engellenememiştir. Sahte e-postaların engellenmesi konusunda e-postalar elektronik imza kullanılarak gönderilmelidirler. Elektronik imzalarda genel (public) ve özel (private) anahtar çiftleri bulunmaktadır. Mail güvenlik cihazları uzman kişiler tarafından yapılandırılmalıdır. Domain bazlı kısıtlama ile sistem güvenliği (örn. ACTIVE DIRECTORY) sağlanmalıdır. Kullanıcılar için yetkilendirilmeler tanımlanmalıdır. Son kullanıcıların bilgisayarlarına sürekli güncellenen anti virüs programları kurulmalı NAC cihazları ile güncellemeler sürekli kontrol edilmelidir.

Periyodik sızma testleri: Periyodik olarak sızma testleri uzman kişiler tarafından yapılmalıdır. Eğer imkanlar el veriyorsa mutlaka bir sızma testi uzmanı çalıştırılması gerekmektedir. Sıfırıncı gün açıklıkları sürekli olarak takip edilmesi gerekmektedir. Açıklıkların kötü niyetli kişilerden önce bulunması, sızma testi uzmanı ile güvenlik ekibinin senkron çalışmaları ile kapatılması kurum veya kuruluşları ileride oluşabilecek risklerden korumak adına atılabilecek çok önemli bir adımdır. Saldırı yapan kişilerin saldırı mantığı ile sistemlere saldıran beyaz şapkalı güvenlik uzmanının bulduğu açıkları raporlaması kurum ve kuruluşlar için hem optimizasyon hem de güvenlik sağlayacaktır.

Gerekli eğitimlerin aldırılması: Sürekli gelişen teknolojinin takip edilebilmesi adına teknik ekibe belli periyotlarda teknik eğitimlerin aldırılması gerekmektedir. Öte yandan çalışan personele uygulamalı olarak farkındalık eğitimlerinin uzman kişiler tarafından verilmesi şarttır. Sosyal mühendislik saldırı yapmak için çok etkili bir silahtır. İnsan faktöründen yararlanan sosyal mühendislik saldırılarının riskinin azaltılması için gerekli farkındalık eğitimleri şarttır.

Uygulama güvenliği: Yazılımların çok uzun kodlardan oluşması, insanların yorgunluğu dikkatsizliği yada bilgi eksikliğinden kaynaklanan açıklıklar mevcut olabilmektedir. Bu açıklıkların kapatılabilmesi için WAF (web güvenlik duvarı), veri tabanı güvenlik duvarı gibi cihazların uzman kişiler tarafından yapılandırılması önemlidir fakat yeterli değildir. Bir yazılımın yapılması aşamasında, yazılım sürekli olarak güvenlik testlerinden geçmelidir. Yazılım kullanılmaya başlandıktan sonra dahi uzman kişiler tarafından periyodik olarak sızma testleri yapılmalıdır. Örneğin web sitesi yazılırken daha yazılma aşamasında güvenlik testleri yapılmalıdır. Web sitesi devreye alındıktan sonra da uzman kişiler tarafından sızma testleri belirli periyotlarda yapılmalıdır ve sıfırıncı gün açıklıkları sürekli takip edilmelidir.

Gerekli politikaların hazırlanması: Kullanıcı, firewall, ağ, sistem, web uygulamaları, yetkilendirme, IPS, IDS sızma testi gibi politikalar hazırlanmalı, hazırlanan bu politikalar kesin bir şekilde taviz vermeden uygulanmalıdır.

Kaynaklar

Resmî Gazete, 2013. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı (Tarih: 20.06. 2013, Sayı: 28683). Erişim Tarihi: 19.11.2013. www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

Baykara, M., Daş, R., Karadoğan, İ. , 2013. Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. 1st International Symposium on Digital Forensics and Security, 20-21 Mayıs, Elazığ, 231-239.

Farkhod Alisherov A., Feruza Sattarova Y., 2009. Methodology for penetration testing, International Journal of of Grid and Distributed Computing, 2(2), 43-50.

Vural Y, ve Sağıroğlu, Ş., 2008. Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2), 507-522.

Rowe, B. R. , Gallaher, M. P., 2006. Private sector cyber security ınvestment strategies: An empirical analysis. The Fifth Workshop on the Economics of Information Security, 26-28 June, England, 1-23

Hoffman, L. J., Rosenberg, T., Dodge, R., Ragsdale, D., 2005. Exploring a national cybersecurity exercise for universities. IEEE Security and Privacy Magazine, 3(5), 27-33

Karaarslan, E., Teke, A., Şengonca, H., 2003. Bilgisayar ağlarında güvenlik politikalarının uygulanması. İletişim Günleri, 29-30 Mayıs,

Ünver, M., Canbay, C., 2010. Ulusal ve uluslararası boyutlarıyla siber güvenlik. Elektrik Mühendisliği Dergisi, 438, 94-103

Akyıldız, M., A., 2013. Siber güvenlik açısından sızma testlerinin uygulamalar ile değerlendirilmesi. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 124s, Isparta.