

Eğitim Kurumlarına Yönelik Sızma Test Metodolojisi

Önder Şahinaslan¹, Ender Şahinaslan², Mesut Razbonyalı³

¹Maltepe Üniversitesi, Bilişim Bölümü

²Bankasya Bilgi Güvenliği

³ Okan Üniversitesi, Mühendislik –Mimarlık Fakültesi, İstanbul

onder@maltepe.edu.tr, ender.sahinaslan@bankasya.com.tr, mesutra@okan.edu.tr

Özet: İnternet eğitim kurumları için vazgeçilmez, önemli bir değerdir. Kıtalar arası anlık bilgilerin taratıldığı, erişildiği, paylaşıldığı elektronik bir kütüphanedir. Bilgi kullanımında akademisyen ve öğrencilerine hız ve rekabet üstünlüğü kazandırır. Ancak bilgi varlıkları üzerindeki yetkisiz erişme, engelleme, değiştirme, hırsızlık gibi risk ve tehditleri de beraberinde getirmektedir[1]. Bu çalışmada, eğitim kurumlarına yönelik temel düzeyde siber tehditlerin önlenmesi amacıyla bir sızma test metodolojisi oluşturulmuştur. Uygulayıcılara katkı ve kolaylık sağlayabilmesi için, BackTrack Open Source yazılımının son sürümü incelenerek uygulama test örneklerine yer verilmiştir.

Anahtar Sözcükler: Eğitim Kurumları, Sızma Testi Metodolojisi, Bilgi Güvenliği, Penetrasyon, BackTrack

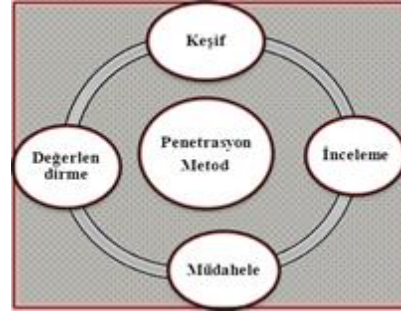
Penetration Testing Methodology for Educational Institutions

Abstract: Internet has an indispensable importance for educational institutions. It is as an intercontinental library to research and share instant information. It gives the quickness and superiority for the usage of information. However, this situation brings the problems on information technology portfolio as the unauthorized access, blocking, substitution and plagiarism. In this study, an infiltration test methodology has been created on the purpose of prohibit the base level cyber threats for the educational institutions. In order to provide convenience and contribution to the users, the last version of BackTrack Open Source software has been observed and given the place to the appliance test examples.

Keywords: Educational Institutions, Penetration Testing Methodology, Information Security, Penetration, BackTrack

1. Giriş

Bugünkü eğitim, öğretim ve yönetim sistemleri eskiye göre daha fazla internete bağımlı hale gelmiştir. Eğitim kurumları siber tehditlere karşı gerçekte, çok büyük risk taşıma potansiyeline sahiptir. Olaya bir üniversite olarak yaklaşıldığında diyebilir ki internetin her boyutu kurumda fazlasıyla kullanılıp test edilebilmektedir. Örneğin laboratuvar ortamlarında incelenmek üzere kurulan yazılımlar her zaman güvenli kaynaktan olmayabilir. Öğrenci atölyelerinde deneme, öğrenme, analiz etme ve merak duygusuyla internetten kurulumlara çoğu zaman müsaade edilmektedir. Bu tür kurulumların sürekli denetim altında tutulması pek mümkün olamamaktadır. Benzer şekilde girilen internet siteleri malware, trojan, virüs eklentileri taşıyabilmekte ve oradan gelebilecek bir uyarıyı öğrenci her zaman dikkate almayabilmektedir. Uzaktan izin ve dosya erişimine paylaştırılmış, portları açılmış, hedefe saldırı aracı haline gelmiş, spam ileti kaynağı, virüs yayan bir makine şekline dönüşebilir. Kısaca bir kampüs ağı internetten gelebilecek zararlı zararsız her türlü yazılım ve uygulamaya hazırlıklı olmalıdır.



Şekil 1 Eğitim kurumlarına yönelik penetrasyon işlem akışı

Bu çalışmayla aynı zamanda, 300 yakın uygulamayı içerisinde bulunduran, açık kaynaklı ücretsiz kurulumu olan bu gelişmiş penetrasyon uygulamasına dikkat çekmeyi amaçlamıştır.

Metodoloji ve Planlama

Eğitim kurumuna ait belirli güvenlik düzeyindeki ihlallerin bulunması ve bu olası ihlallerin ortadan kaldırılmasına yönelik metodun planlanma aşamasıdır. Gerçek bir saldırgan gibi senaryo oluşturulmalıdır. Planlamada, bir eğitim kurumuna ait potansiyel güvenlik açıklıklarına neden olabilecek bilgi varlıkları tespit edilir.



Şekil 2. Varlıklar üzerinden bilgi toplama

Başarılı bir test, şekil 2’de belirtilen süreçler üzerinden profesyonel senaryolar oluşturularak elde edilebilir. Şekil 1’de oluşturulan döngü üzerinden işlem basamakları oluşturulabilir. Bilgi varlıklarının keşfetme, açıklıkları bulma ve inceleme, tespit edilen açıklıklara müdahale, sonrasında yeniden test edip değerlendirme şeklinde bir metod takip edilmelidir. Kurgulanan saldırı senaryoları gerçeğe yakın olmalıdır. Bu nedenle senaryo içerisinde görev ve roller iyi tanımlanmalıdır[3]. Test sırasında olası sistem aksaklıkları ve işlem kesintileri yaşanmaması için kim nerede görev almalı, anında geri dönüşler için son sistem yedekler alınmalıdır. Test işlemi için sistemin yoğunluk durumuna karşı uygun zamanlama seçilmelidir.

Bilgi Varlıkları Üzerinde Keşif ve Zaafiyet Tarama
Bir eğitim kurumunda risk oluşturacak güvenlik açıklıklarının taranması işlemidir. Buradaki amaç penetrasyon test yapmak için ihtiyacımız olan bilgileri elde etmektir. Uzaktan sistem kaynakları üzerinde okumayazma yetkisini elde etmeyi test eder[4]. Güvenlik testine başlandığında ilk aşama olarak hedef eğitim kurumu hakkında mümkün olduğu kadar çok bilgi toplamak gerekir. Şekil 3’de Backtrack yazılımı üzerinde gelen ve gruplandırılmış bilgi toplama araçları ile ağ, web tabanlı uygulama, veritabanı ve kablosuz erişim bileşenleri hakkında araştırma yapmamızı sağlar.

3.1. Keşif ve Haritalama

Bilgi toplama bir Penetrasyon testinin en kritik adımudur. Başlangıçta zaman kaybı gibi görünse de test esnasında bize yardımcı olacak bilgiler bu aşamada toplanmış olmalıdır. Sistemde çalışan sunucular, güvenlik duvarı, aktif cihazlar gibi sistem elamanları tespit edilir. Nmap pek çok parametreye sahiptir. Ağ haritalamada da oldukça etkin kullanılır.

```
# nmap [tarama türü] [seçenekler] {hedef}
```

Açık portlar, çalışan servisler, işletim sistemleri, tanımlı host bilgileri elde edilebilir. Ayrıca arama motorlarından istifade edilir. Test işlemini kolaylaştırmak için ağ şeması ve bilgi sistemleri ile ilgili elde edilen tüm bilgiler ve ağ şema yapısı haritalanmalıdır. Bunun için en önemli haritala oluşturma yazılımı Maltego ’dur. BackTrack-Information Gathering-Network Analysis-DNS Analysis –Maltego alt menüsünden çalıştırılabilir. Aynı zamanda terminal penceresinden komut satırı kullanılarak çalıştırılmak mümkündür.

- Aktif Bilgi Toplama
- Pasif Bilgi Toplama
- İnternete Açık Servisler Üzerinden Bilgi Toplama
- Arama Motorlarını Kullanarak Bilgi Toplama
- Maltego üzerinden Bilgi Toplama



Şekil 3.7 Maltego ile ağ haritası oluşturma

Şeklinde keşif ve haritalama süreçleri tamamlanmış olur. Ayrıca bir siteye bağlı alt domainler, e-postalar, TCP port ve IP taramaları için” Dmitry” yazılımı kullanılır.

```
root~# dmitry -wn -o sorgu.txt xyz.com
```

-w: Whois sorgusu yapar

-n: Netcraft bilgisini verir

-o : Taranan bilgileri belirtilen txt dosyasına yazar.

3.2. Sosyal Mühendislik

Sosyal mühendislik günümüz güvenlik dünyasının en yaygın zaafiyet yöntemi haline gelmiştir. Saldırının başarısı tamamen insan faktörüne dayanmaktadır. İnsan doğası gereği her zaman hata yapmaya hazırdır. Bilinen etkin kullanıma sahip 300 e yakın sosyal paylaşım sitesi(Facebook, Twitter MySpace, Friendster..) ve bloglar(Xanga ve Blogspot..Such sites enable users to create online profiles and post pictures) vardır. Saldırganlar bu kanallar üzerinden farklı kimliklerle yalan, hile, rüşvet, şantaj gibi tehditlerle bilgi elde etmektedirler[6]. Penetrasyon testlerinde o eğitim kurumuna ait sosyal medya üzerinden hangi bilgilerin elde edildiği araştırılır. Çalışma ofisi, çalışma masası, ekranın, klavyenin, yazıcının çevresi küçük notlar şeklinde şifre, kullanıcı adı, IP vb. kritik bilgiler yönünden araştırılır. Sistemcilerin yanında durulduğunda şifreler açık görülür şekilde mi giriliyor.



Şekil 3.2.a İzleme yöntemi kullanılarak yapılan sosyal mühendislik

Kritik pozisyonda çalışanlara ait profil bilgileri, hobileri, aktiviteleri, sosyal arkadaş bilgileri, tatil, izin ve ailevi bilgileri toplanır. Elde edilen bu dost bilgilerine benzer isimlerle e-posta oluşturup bilgi elde etmeye yönelik rica, sahte program kurduklarında e-posta ve mesajlarla tuzağa düşürülme testi yapılır. Eposta ve web sayfası sahteciliği sosyal

mühendislik saldırılarının en önemli adımlardan bir tanesidir. Hedef kurbanın bilgisayarını ele geçirmeye veya hazırlanan sahte web sayfasına çekmeye çalışır. İnternette istihbaratların %80'ni açık kaynak olarak formlarda yayınlanan bilgilerden elde edilir. Özellikle sistem yöneticilerinin internette atacağı her adım, paylaşacağı her bilgi saldırganlar için çok değerlidir[<http://www.social-engineer.org/>].



Şekil3.2.b Sosyal mühendislik tarama araçları

Social Engineering Toolkit (SET) Backtrack içerisinde sosyal mühendislik tarama araçlarını kapsar. İçerisinde kullanılan yazılım araçları ile insan zafiyetleri üzerine oluşturulmuş hazır senaryolarla olası açıklıklar test edilmiş olur. E-postalar, şüpheli web bağlantıları, online anti-virüs mesajları ve video codec güncellemeleri gibi bilinmeyen linkler ve tehlikeleri test yapar.



Şekil 3.2.c Sosyal mühendislik tarama listesi

Şekil 3.2.c de bulunan sosyal mühendislik saldırı seçeneklerinden yapılmak istenen saldırı test türü seçilir. Websecurify, Metasploit, Meterpreter açık kaynaklı yazılım araçları kullanılır. It can be very hazardous to your network.

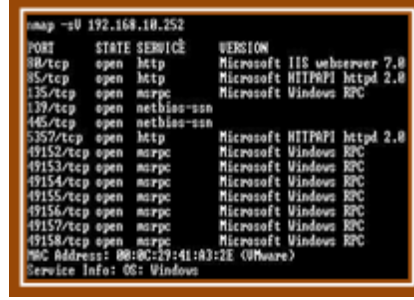
3.3. Port Açıklıkları

İnternete bağlı sistemler üzerinde çalışan servislere ait aktif portlar ve pasif portlar tespit edilir. Açık portların durumu sorgulanır. İlgili portun bir servisle ilişkilendirilme durumu incelenir. Bu portlar üzerindeki bilinen zafiyetler test edilir. İlişkilendirilmemiş boştaki açık portlar derhal kapatılır. Zafiyet tarama araçlarından en bilineni nmap'dir.

```
#nmap -p -sV 1-500 192.168.1.1
```

Hedefteki IP nolu makinada 1-500 arası portları tarar. Açık-kapalı olma durumları hakkında bilgi verir. -p ve port numaraları yerine doğrudan -r parametresi

verilirse ilgili IP deki makinanın portları 1 den başlanarak sırasıyla taranır.

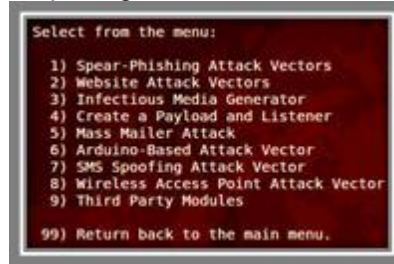


Şekil 3.3 Nmap ile port tarama örneği

Şekil 3.3 de tarama sonucu görülmüş bu komut satırıyla da belirtilen IP deki bir makinanın -sV parametresi ile açık olan tüm portlardaki çalışan servis uygulamaları ve sürümleri hakkında bilgi verir.

3.4. Ağ Cihazları

Kablolu veya kablosuz ağa dâhil olan tüm aktif cihazlar standart güvenlik denetimlerine tabii tutulur. Özellikle yönlendirme özellikleri bulunan router, omurga veya akıllı diyebileceğimiz programlanabilir switch'lere konsol dan veya uzaktan erişim yetki kazanabilme oldukça önemlidir. Aynı şekilde güvenlik duvarı ve üzerindeki tanımlamalar, kurallara erişim, konfigürasyonun görünebilmesi, eksik kural tanımlama veya yanlış yapılandırılmış cihazlar ağ üzerinde zafiyetlere neden olur. Genelde ağ cihazları güvenlik tarafında yapılandırılırken genelde saldırının yerel ağı dışından geleceği gibi düşünülür. Daha çok güvenlik duvarı üzerinde durulur. Fakat içerideki kullanıcıların aktif cihazlara erişim için tedbir almak pek düşünülmez. Bu cihazlardaki erişim güvenliği ve yapılandırılması oldukça düşüktür. Yapılan araştırmalar pek çok saldırının aslında yerel bağlantılar üzerinden gerçekleştiğini ortaya koymuştur. Bu nedenle eğitim kurumlarında ağ üzerinde yapılacak bir penetrasyon testi olası zafiyetleri gün yüzüne çıkaracaktır. Önleyici tedbirlerin alınmasına vesile olacaktır. Test amaçlı yine backtrack yazılımı içerisindeki "Network Analysis" başlığı altında 10 dan fazla alt bileşene ayrılmıştır. Şekil 3.4 de bu bileşenler görülmektedir.



Şekil 3.4 Ağ erişim tarama test araçları

Örneğin "Network Scanner" altında autoscan komutu çalıştırılarak ağa bağlı olan ekipmanları IP numaraları ile birlikte listesini oluşturur. Daha sonra bu cihazlar üzerinde nmap parametreleri kullanılarak açık portlar ve zafiyetler üzerinde inceleme gerçekleştirilir.

3.5 İşletim Sistemleri

Özellikle sunuculardan başlamak üzere ağda kullanılan işletim sistemleri tespit edilir. Bunların güncel olup olmadıkları versiyon numaraları takip edilerek bulunabilir. Yama ve güncelleştirilmemiş bilgisayarlar zafiyet göstergesidir. İşletim sistemi bilgisi nmap komutu kullanılarak "o" parametresi işletim sistemini "A" parametresi ile de ayrıntılı bilgi elde edilir.

```
root@bt~# nmap -o -A hedef ip numarası
```

Günümüzde halen çok fazla kullanılan açıklık son service pack yaması yapılmamış Windows XP yüklü bilgisayarlardaki MS08-067 zayıflığı. Bu zafiyet kullanılarak Metasploit yazılımı ile hedef bilgisayar ele geçiriliyor.

3.6 Yazılım ve Veri tabanları

Özellikle internet tabanlı güçlü yazılımlar, arkasında gelişmiş bir veritabanı uygulamasına ihtiyaç duyar. Gerçekte veri havuzu veritabanı üzerinde tutulur. Bu servise erişim, yetkilendirme, tutulduğu sunucu ve işletim sistemi, fiziki erişim güvenlik açısından oldukça kıymetli ve kritik durumdadır. Veri tabanına kimler ne şekilde erişti ve ne tür değişikliklerin yapıldığı log bilgisi mutlaka tutulmalıdır.



Şekil 3.6 Veritabanı zafiyet araştırma araçları

Web sitelerinde kullanılan kodlardan ve dosyalardan kaynaklanan zafiyetleri ortaya çıkartır. Örneğin SQL injection açıklığı ve XSS zafiyeti acunetix test tarayıcısı ile bulunabilir.

3.7 Web Uygulamaları

Eğitim kurumlarında online işlem sayfaları öğrenci ve akademisyenler tarafından artan bir eğilimle tercih edilmektedir. Kayıt işlemleri, not işlemleri, muhasebe işlemleri, ders seçmeler, elektronik haberleşme servisleri, ödev ve dosya paylaşım portalları bunlardan bazılarıdır. Kullanıcı adı ve şifre doğrulaması gerektiren tarayıcıların HTTPS bağlantısı üzerinden gerçekleşmesi gereklidir. Web sunucular SQL açıklıkları, Cross Site Scripting açıklıklarına karşı test edilir. Ayrıca DDOS saldırılarına karşı dayanıklılık testine tabi tutulur.

Web uygulamaları OWASP'ın yayınladığı Top 10 açıklıklarına karşı test edilir. Web Servisleri SQL, LDAP, OS ve XPATH zehirleme ve arabellek taşması şeklinde saldırı düzenlenebilir[5].



Şekil 3.7 Web uygulamaları test araçları

Yukarıdaki şekilde belirtildiği gibi BackTrack yazılımı içerisindeki açık kaynaklı araçlar bir eğitim sitesi web Penetrasyon testi için yeterlidir. Eğitim kurumuna ait web uygulamaları güvenlik açıklık ve risklere karşı zafiyet sınavına tabi tutulur.

4. Zafiyet Sonuçları ve İnceleme

Eğitim kurumlarındaki güvenlik olayları tespit edildikten sonra bunlara karşı alınması gereken müdahale süreçleri belirlenir. Güvenlik duvarı ve üzerinde tanımlanan kuralların güncelliği ve olası açıklıklar yazılım araçları ile analiz edilir. Sunucuların hem iç ağ hem de dış ağdan gelebilecek tehditlere karşı açıklık sonuçları test edilir. Kısaca kablolu/kablosuz ağ, cihazları, web uygulamaları, veritabanı, sosyal ağ, fiziksel güvenlik gibi bileşenler üzerine yapılan zafiyet araştırma sonuçları birleştirilir. Bunlar üzerinde tespit edilen açıklıklar aşağıda belirtilen yöntemlerle tek tek gerçeklik testine tabi tutulur[4].

4.1 Zafiyet Gerçeklik Testi ve Müdahale

Daha önce yapılan test taramadan elde edilen açıklık sonuçlarının gerçekliğinin araştırılmasıdır. Yani açıklığa özgü exploit işlemine tabi tutularak açıklığın risk durumu analiz edilmiş olur. BackTrack içerisinde bulunan Exploitation Tools araçları bu işlem için kullanılır[7].



Şekil 4.1. Zafiyet gerçeklik test araçları

Açık kaynak kodlu bir test aracı olan Metasploit, Perl programlama dilinde yazılmaya başlanmış fakat daha sonra Ruby dili ile yeniden geliştirilmiş bir zafiyet tespit ve exploit aracıdır. Saldırganlar, anti virüs

geliştiricileri ve pentest uzmanlarının sıklıkla kullandıkları yazılım aracıdır. Metasploit, set edilen payload'ların encode edilerek sistemlere gönderilebilme yeteneğine sahiptir. IPS/IDS gibi saldırı tespit ve engelleme sistemlerini atlatarak, anti virüs ve kişisel güvenlik duvarlarına takılmadan uzak sistemler üzerinde çalıştırabilme özelliğine de sahiptir. Metasploit ile çalışmak için temel olarak şu 3 adım gerçekleştirilir:

- Hedef sistem sunucularında veya kullanıcı bilgisayar işletim sistemi üzerinde çalışacak uygun exploit'itespiti ve gerekli konfigürasyonunun yapılması
- Bulunan zafiyete uygun payload'un belirlenmesi ve konfigürasyonunun yapılması
- Exploit işleminin gerçekleştirilmesi
- Metasploit, tarayıcı tabanlı açıklıkların kullanılmasına özgü içerisinde birçok yazılım aracı bulundurulur. Örneğin test esnasında Metasploit kullanılarak kötü amaçlı bir web sunucusu gibi davranarak kullanıcıları tuzağa çekebilir.

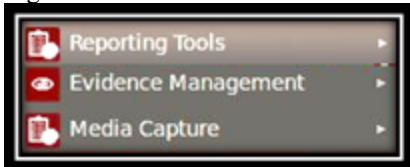
4.2 Değerlendirme

Eğitim kurumuna ait tüm bilgi kaynakları üzerinde güvenlik açıklıkları, tasarım zayıflıkları ve riskler bu şekilde yapılacak penetrasyon testi ile ortaya çıkartılmış olur. Bu işlem o kuruma karşılaşılabilecekleri bir siber tehdit karşısında hazırlıklı olmayı, iş devamlılığının aksamamasını sağlar. Bu test aynı zamanda cihazların güvenli olmayan yanlış yapılandırma hatalarını da ortaya çıkartır. Başarılı yapılan testler ve sonrasında açıklıkların kapatılması sayesinde kurumun, öğrencilerin ve personelin bilgi varlıkları korunmuş olur. Olası kurumsal itibar ve maddi kayıplar engellenmiş olur. Kurumun yapmış olduğu güvenlik yatırımları bu şekilde zafiyet testinden geçirilmiş olur[8].

Eğitim kurumlarında ağ ve bilgi güvenliği sorumluları başta olmak üzere yazılım geliştirme ve teknik personellerin güncel siber formları takip etmeleri ve son saldırı ve veri sızma tekniklerinin neler olduğunu izlemelidirler. Kuruma özgü güvenlik politika belgesi oluşturularak, yeni ihtiyaçlar dâhilinde sürekli güncel tutulmalıdır. Yazılı güvenlik kurallarına mutlaka uyum sağlanmalıdır[9].

4.3 Raporlama

Güvenlik uzmanları tarafından penetrasyon testlerinde en fazla kullanımı olan backtrack içerisinde raporlama amaçlı Şekil 4.3 de görülen Reporting Tools başlığı altında toplanmıştır. Pentest çalışmalarından elde edilen sonuç değerlerini kullanarak rapor oluşturmayı sağlar.



Şekil 4.3 Pentest raporlama araçları

Açık kaynak yazılım uygulaması olan bu raporlama araçlarından grafik ara yüzü kolay kullanıma sahip Dradis tercih edilmektedir. Konsoldan #./start.sh komutu ile Dradis başlatılır. Grafik ekranından kullanmak için <https://localhost:3004> adresi tarayıcıdan girilir. Ekranı çıkan sertifika doğrulaması ve şifre oluşturma ekranları tamamlanır. Nmap, Nessus gibi zafiyet test tarama çıktıları doğrudan -oX parametresi kullanılarak .xml uzantılı bir dosyaya aktarılır. Oluşan bu dosya Dradis'e import from ara yüzünden aktarılarak tekrar incelenmek üzere düzenli raporlar oluşturulur.

Ayrıca elde edilen zafiyet risk oranları düzenli olarak takip edilerek uygulama-zafiyet ilişkileri çıkartılır. Tespit edilen zafiyetler kritik seviyelerine göre "acil, kritik, yüksek, orta, düşük" şeklinde kategorize edilir. Bunların bir eğitim kurumunda sistemlere göre dağılımları da yapılarak teknik kişiler ve yönetimin bu zafiyetler konusunda bilgilendirildiği detaylı raporlar oluşturulur[10].

5. Sonuç ve Öneriler

Eğitim Kurumlarının yetkisiz kişiler tarafından kritik verilerini tehdit edilebilme durumuna karşı yılda en az bir defa penetrasyon testi yapılmalıdır. Sunucu sistemleri üzerine yeni bir donanım veya yazılım ilave edildiğinde özellikle bu değişimi hedef alan testler gerçekleştirilmelidir[11]. Bu sayede bize olası bir saldırının nereden gelebileceğini ve gerçekten ağır ve verilerin korunaklı olup olmadığı hakkında öncesinde fikir verir.

Kurum bu çalışmada planlandığı şekliyle içeriden ve dışarıdan bir saldırı testlerine tabi tutularak zafiyet durumu araştırılır. Olası bir zafiyetin ne derece kullanılabilir olduğu ve hangi sistem varlıklarına kadar erişebildiği tespit edilmiş olur[12]. Bu alanda geliştirilmiş pek çok açık kaynak kodlu yazılım bulunmaktadır. Benzer bir testi kurumda yapacaklara kolaylık olması açısından bildiri de bunların pek çoğunu üzerinde bulunduran ücretsiz BackTrack yazılımı örneklendirildi. Bu konuda <http://www.backtrack-linux.org>,

<https://www.owasp.org>, <http://www.eccouncil.org> sitelerinin oldukça yararlı olacağı düşünülmektedir.

Çok iyi korunduğu düşünülse dahi, alınan güvenlik önlemlerinin ne kadar etkili olduğunu analiz edilmesi ve gözden kaçan olası reel açıklıkların da görülmesi ve tedbir alınmasına katkı sağlar. Bütün bu avantajlarının yanı sıra siber saldırılara maruz kalmamak için eğitim kurumlarında da mutlaka penetrasyon testlerinin yapılması karşı tedbirlerin alınması önerilmektedir.

Ayrıca eğitim kurumlarının araştırma ve geliştirme felsefesine uygun bir platform olan açık kaynaklı yazılımlar her geçen gün gelişerek daha da yetenekli hale gelmektedir. Bu yazılım üniversite düzeyinde laboratuvar ortamlarında bir proje olarak ele alınabilir. Bu sayede mezun öğrencilerden ilgi duyanların siber güvenlik alanında uzman olarak iş bulmasına katkı sağlayacaktır.

6. Kaynaklar

- [1] BackTrack Linux - Penetration Testing Distribution. BackTrack 5 R3 Released! Aug 13th, 2012 www.backtrack-linux.org
- [2] TUBITAK, BOME 2008 Bilgi Sistemleri Güvenliği Tatbikatı.3.3 Kurulum Adresi, <http://www.bilgiguvenligi.org>, (2012)
- [3]Ö.Şahinaslan,M.Razbonyalı,E. Şahinaslan “Akıllı Şehirlerin Tasarımında Yedi Adımda Siber Güvenlik”. VI. İstanbul Bilişim Kongresi “Akıllı Yaşam Ve Başarı Örnekleri: Akıllı Şehirler” 7-8 Kasım 2012-İstanbul
- [4]A.Shakeel, T.Heriyanto BackTrack 4: Assuring Security by Penetration Testing Copyright,2011 Packt Publishing S.333
- [5]The Open Web Application Security Project(OWASP)–2012
<http://owasp.com/index.php/>
- [6]Ö Şahinaslan, E Şahinaslan M Razbonyalı, Open Source Administration Software and Implementation Results for Ensuring Electronic Communication and Information Security Gediz University ISCSE 2010, Kuşadası, S.3
- [7] The Exploit Database (EDB). Offensive Security 2012 <http://www.exploit-db.com/>
- [8]Cynergi Solutions Inc. Eclipse Bank PLC Penetration Report-July 2012 <http://digitalencode.net/>
- [9]Bilgi Güvenliği Akademisi (BGA) <http://www.bga.com.tr/> - 2012
- [10] EC-Council University is An Academy of Teachers and Learners – 2012<http://www.eccuni.us/Academics.aspx>
- [11] K.Demirez, “Linux BackTrack 5” Nirvana Yayıncılık. Eylül-2011, S.89-325
- [12] Gupta, Manish, John Walp ve Raj Sharman. Threats, Countermeasures, and Advanced in Applied Information Security" Tehditler, Karşı, ve Uygulamalı Bilgi Güvenliği Gelişmeler." IGI Global, 2012. 0-319. 20 Nisan 2012.