Ülkemizdeki Üniversite Web Sayfalarının Siber Güvenlik Açısından Hızlı Bir Değerlendirmesi

Kadriye Huysal Özgöçmen[1], Baran Çelik[1], Halil Özgür Baktır[1]

[1] İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Enformatik Bölümü, İstanbul

kkhuysal[at]gmail.com, baran.celik[at]gmail.com, ozgur.baktir[at]gmail.com

Özet: Ülkemizde Siber Güvenlik konusu, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının [1] Resmi Gazetede yayımlanması ve bu eylem planındaki ilkelerin hayata geçmeye başlaması ile hak ettiği önemi kazanmış durumda olup her geçen gün Siber Güvenlik konusuna verilen önem daha da artmaktadır. Eylem Planı incelendiğinde üniversitelerimize hem siber güvenlik konusunda yetkin personel yetiştirilmesi ve bilgi güvenliği farkındalığının artırılması, hem de bilgi ve ürün geliştirilmesi gibi görevler atfedilmiş olup üniversitelerimizin konuyla ilgili lokomotif konumunda yer aldıkları görülmektedir. Bu çalışmada üniversitelerimizin internet ana sayfaları baz alınarak iki temel referans üzerinden siber güvenlik konusundaki mevcut durum ve farkındalık resmedilmeye çalışılmıştır. Çalışmada uygulanan yöntemler yasal sınırlar içerisinde kalmakta olup bu sınırları aşarak kişiler veya sistemler tarafından saldırı olarak algılanabilecek uygulamalardan ve hassas/kişisel bilgilerin ifşasından özellikle kaçınılmıştır.

Anahtar Sözcükler: Siber Güvenlik, Web Sunucu Güvenliği, Web Güvenliği, Siber Saldırı, Veri Toplama, HTTP Parmak izi Taraması (HTTP Fingerprinting), E-posta Hasadı (E-mail Harvesting).

Abstract: In our country, after the publication of National Cyber Security Strategy and Action Plan 2013-2014 in the Official Journal and starting realization of the principles of this action plan, cyber security issues have gained its deserved importance and with each passing day the importance given to cyber security issues is increasing. When Action Plan is analyzed tasks such as training qualified person in cyber security, increasing the awareness of information security, developing of information and products have been attributed to our universities and universities position on the subject can be seen that the locomotive. In this study, current situation and awareness about cyber security has been tried to describe over the two fundamental references, based on our universities' web homepages. The methods used in this study remain within legal limits. Beyond the legal limits, applications which may be perceived as offensive by people or systems and disclosure of personal/sensitive information have been especially avoided.

1. Giriş

Başlangıçta temel amacı askeri ve akademik ortamdaki iletişimi sağlamak olan İnternet, günümüzde kolaylık sağlayan bir araç olmanın çok ötesine geçip, iş ve bireysel hayatın ayrılmaz bir parçası olmuş ve böylelikle kullanılması zorunlu bir vasıta halini almıştır. Özellikle mobil cihazlar ve mobil internet kullanımı birçok sınırı ortadan kaldırmıştır. Gündelik hayatın internet ile bu ölçüde bütünleşmiş olması, bilgilerimizin güvenliğini ve işlerimizin sürekliliğini de aynı ölçüde tehlikeye sokmaktadır. Kamu kurumlarındaki gizli bilgiler, enerji, su, ulaşım gibi hayatı idame ettirmek için gereken kritik altyapılar düşünüldüğünde tehlikenin büyüklüğü ve konunun hassasiyeti daha iyi anlaşılmaktadır. Siber ortamda, olayların saniyelerle ifade edebilecek zaman dilimlerinde meydana geldiği de göz önünde bulundurulursa etkin ve güçlü bir siber savunmanın inşası, farkındalık ve bilinç oluşturmanın önemi daha bariz bir biçimde ortaya çıkacaktır.

2. Bir Saldırının Anatomisi

Siber suçların sayısı ve şiddeti artmaya devam ettikçe, siber suçluların ağlara saldırmak için kullanabilecekleri saldırı yöntem ve adımlarının, zararlı yazılım türlerinin ve onları durdurmak için ihtiyaç duyulabilecek araçların biliniyor olması da önem kazanmaktadır.

Genel kanının aksine saldırganlar istedikleri sisteme istedikleri zaman girip keyiflerince dolaşamazlar. Bir sisteme sızmak için ciddi bir stratejinin uygulanması gerekir.

Bir siber saldırının anatomisi, keşif (hedef hakkında bilgi toplama), tarama (güvenlik açıklarını bulma), erişimi sağlama (saldırma, sızma, ele geçirme, etkisiz kılma, zarar verme), erişimi devam ettirme (kötücül yazılım gizleme) ve izleri temizleme fazlarından oluşmaktadır.

Şekil 1. Bir Saldırının Aşamaları

Keşif fazında saldırgan hedef hakkında (hedefe ait alan adları, IP adres aralığı, aktif sistemler ve bu sistemler üzerinde çalışan işletim sistemleri, servisler/hizmetler ile yama seviyeleri, çalışanlar, çalışanların e-posta adresleri gibi) bilgiler toplar.

Tarama fazında hedef sisteme ait açık servisler, portlar, istismar edilebilecek işletim sistemi açıkları tespit edilir. (örnek olarak Nmap programı kullanılarak yapılabilecek taramalar verilebilir.)

Saldırı fazında önceki aşamalarda toplanan bilgiler kullanılıp istismar edilerek hedef sisteme sızmaya çalışılır. İşletim sistemi ve ara bellek istismarları, ağ saldırıları (dinleme, zehirleme, araya girme teknikleri) bu aşamada kullanılan bazı yöntemlerdir.

Erişimi devam ettirme fazında ise ele geçirilmiş sistemde arka kapılar (backdoor), Truva atları (trojan) bırakılarak istenilen zamanda erişim ve istismar sağlanmış olur.

Son aşama olan izleri silme fazında ise saldırıya ve saldırgana ait veri tespitinin önüne geçecek şekilde saldırı izlerinin hedef sistemlerden silinmesi veya mevcut varlığın gizlenmesi şeklindedir.

Çalışmanın odak noktasını oluşturan ve bir saldırının ilk aşaması olan keşif aşaması, yöntem açısından üç farklı alt grup halinde sınıflandırılabilmektedir.

Şekil 2. Keşif Fazı (Reconnaissance)

Pasif Keşifte hedef, saldırgan tarafından yapılan işlemden habersizdir. Hedef ve saldırgan arasında veri akışı yoktur. (Google Aramaları, Whois Sorgusu, vb.) Yarı-Pasif Keşifte hedef, saldırgan tarafından yapılan işlemden haberdardır. Hedef ve saldırgan arasında olağan (normal) bir veri akışı vardır. (HTTP Parmak izi taraması, vb.) Aktif Keşifte hedef, yapılan işlemden haberdardır. Hedef ve saldırgan arasında olağandışı (anormal) bir veri akışı vardır (NMAP Taraması, vb.)

Pasif Keşif (Passive Reconnaissance) aşamasında birçok farklı kaynaktan farklı yöntemlerle farklı türden bilgi keşfi mümkün olup aşağıda bu aşamaya ilişkin bazı örnekler verilmiştir.

- ***IP Adres ve alt alan adlarının keşfi*** (Whois sorguları, Google aramaları, Netcraft vb. sayfaların kullanılması, web sayfalarının görüntülenmesi ve sayfalarda dallanma - Browsing/Spidering)
- ***İlgili kişilerin keşfi*** (E-posta hasadı, Maltego gibi araçların kullanılması, hedef web sayfaları, Linkedin gibi 3.parti veri kaynakları, mesaj tahtaları, kullanıcı forumları, sosyal medya sayfaları, Spokeo/Pipl gibi kişi arama sayfaları ve doküman üst verilerinin incelenmesi)
- ***Kullanılan teknolojilerin keşfi*** (HTTP parmak izi tarama, Wappalyzer, Whatweb gibi araçların kullanılması, Shodan arama motorundan faydalanma, dosya uzantıları (php, asp, jsp, cfm, vb.), sunucu cevapları, iş ilanları, dizin listeleme, bilgilendirme sayfaları, oturum açma sayfaları, web sayfası içerikleri, kamuya açık ihale ilanlarının incelenmesi ve dokümanların taranması)
- ***İlgili olabilecek içeriğin keşfi*** (dışa açık web portali, web e-posta ara yüzü, yönetici panelleri, test sayfaları, log dosyaları, yedek dosyalar, zamanı geçmiş dosyalar ve sunucu tarafındaki kodlar, yapılandırma dosyaları, veri tabanı döküm dosyaları, istemci tarafı kodlar, kullanıcı adı ve şifre dosyaları, web servis tanım dil dosyalarının incelenmesi)
- ***Zafiyetlerin keşfi*** (keşfedilen teknolojiler ile ilgili bilinen zafiyetlerin araştırılması, URL denemeleri, vekil sunucu üzerinden pasif taramaların yapılması, hata mesajlarının gözden geçirilmesi) [2]
- Çöp karıştırma (dumpster diving / garbage picking) yöntemiyle herhangi bir türden bilgi keşfi (erişim, IP, ilgili kişi vb. bilgilerinin elde edilmesi)

3. Çalışmanın Kapsam ve Yöntemi

Bu çalışma daha öncede belirtildiği gibi saldırı amacı gütmeyip bir siber saldırının ilk aşaması olan keşif aşamasında elde edilen veriler üzerinden ülkemizdeki üniversite web sayfalarının siber güvenlik açısından hızlı bir değerlendirmesini yapmayı hedeflemektedir.
Günümüzde bir web sayfası önemli ticari bilgiler içermiyor veya kritik hizmetler vermiyor olsa bile saldırganlar tarafından egolarını tatmin etmek ya da isimlerini duyurmak için bozguna uğratılabilmekte (defacement), böylesi bir durumda ilgili kurumun itibarı zedelenmekte, marka değeri düşmekte ve zaman zaman da ticari kayıplar oluşabilmektedir.

Açık kaynaklardan çevrimiçi toplanan veya doğrudan anonim olarak raporlanan bilgileri arşivleyerek web sayfalarına ait bozgun istatistiklerini tutan Zone-H [3] sitesinde "edu.tr" uzantılı domainler için küçük bir arama yapıldığında 2.933 adet bozgun kaydı bulunduğu görülmekte olup bunların 1.100 adedi son 4 yıla ait olan kayıtlardır.

Bu çalışmada YÖK [4] web sayfasındaki 196 adet üniversite web ana sayfası linki ve domain adresleri girdi olarak alınmıştır.

Çalışmada bir siber saldırının ilk aşaması olan keşif/tanıma aşamasında kullanılabilecek iki temel yöntem, üniversite web linkleri (ana sayfaları) üzerine uygulanarak siber güvenlik durumları ve dolayısı ile bilgi güvenliği farkındalığı analiz edilmeye çalışılmıştır.

Çalışmada kullanılan yöntemler günlük hayatta sıradan bir son kullanıcının web hizmetinden faydalanması için gerçekleştirdiği işlemler ve elde ettiği çıktılarla sınırlı olup yasal sınırlar dâhilindedir. Bu sınırları aşarak kişiler veya sistemler tarafından saldırı olarak algılanabilecek uygulamalardan ve hassas/kişisel bilgilerin ifşasından özellikle kaçınılmıştır.

3.1. HTTP Parmak izi Taraması (HTTP Fingerprinting)

Genel manada parmak izi taraması, belirli amaca yönelik olarak hedef cihazdan veri toplama işlemi olarak yorumlanabilir.

Cihazlarda gerçekleştirilen parmak izi taramanın arka planındaki motivasyon parmak izinin adli bir değerinin olmasından kaynaklıdır. Parmak izi mantığından hareketle ideal durum söz konusu olsaydı tüm web istemci makineleri farklı bir parmak izi değerine sahip olurdu (farklılık - diversity) ve bu değer değiştirilemezdi (değişmezlik-stability). Böylesi bir durumda da bir ağdaki tüm cihazları birbirinden ayırt edebilmek mümkün olurdu. Gerçekte farklılık ve değişmezlik ilkeleri aynı anda tam olarak sağlanamamakta, bir ilkenin tam olarak sağlanmaya çalışılması durumunda diğer ilke olumsuz yönde etkilenmektedir.

Parmak izinde farklılık ilkesi, aynı parmak izine sahip birden fazla cihaz olmamasını gerektirir. Yani her cihazın eşsiz bir parmak izine sahip olması gerekir. Ancak gerçekte çok sayıda cihaz üretim esnasında yüklenen işletim sistemlerinden kaynaklı olarak hemen hemen aynı yapılandırmaya dolayısıyla da yaklaşık olarak aynı parmak izine sahip olmaktadır. Parmak izlerinin neredeyse birebir aynı olduğu böylesi durumlarda istemci cihazlardan daha fazla sayıda parametre toplayabilecek bir betik dil kullanılabilir ancak bu defa da zamanla değişikliğe uğramış olma ihtimali olan parametrelerden kaynaklı olarak parmak izinin değişmezlik ilkesi tam olarak sağlanamamış olacaktır.

Parmak izinde değişmezlik ilkesi ise zaman içerisinde aynı kalmayı gerektirir. Bununla birlikte tarayıcı yapılandırma tercihlerinin değiştirilemez olmaması nedeniyle tarayıcı tarafındaki çerezlerin durumunun kapalı ya da açık olması gibi basit değişiklikler bile parmak izinin değişmesini sağlayabilmektedir. Değişmemiş olduğu bilinen ya da tahmin edilen daha az sayıdaki parametreyi toplamak bu duruma bir çözüm olabilir ancak bu durumda da farklılık ilkesi tam olarak gözetilememiş olacaktır. [5].

HTTP parmak izi taraması (HTTP Fingerprinting) HTTP sunucuya gönderilen taleplere karşılık olarak sunucudan gelen HTTP yanıt mesajlarının karakteristiğinin analizi yoluyla HTTP sunucu kimlik bilgisinin, parametrelerinin belirlenmesi işlemidir. HTTP sunucu tarafında özel yapılandırmalarla bazı HTTP parmak izi tarama yöntemlerinden kaçınılabilir. Ancak HTTP parmak izi tarama ile web sunucular hakkında veri toplamak her zaman için

mümkün olabilmektedir. Sunucu tarafındaki özel yapılandırmalar ile sadece veri toplama işlemi zorlaştırılabilmektedir (hardening). HTTP parmak izi taramada Amap, Netcat, HMAP, httprint vb. programlar kullanılmakta olup NMAP programı ile birlikte kullanıldığında daha güvenilir sonuçlar elde etmek mümkün olabilmektedir. [6]

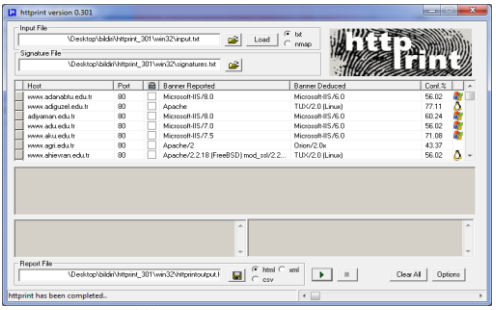
Web tarayıcılar, internet sayfalarına bağlanırken HTTP'nin doğası gereği HTTP mesaj başlıklarındaki bazı parametrelerden faydalanarak sunucu hakkında bazı bilgiler edinirler. Bu işlem, HTTP parmak izi elde etme amacıyla da kullanılabilmektedir. Tarayıcılar web sayfalarına bağlanırken daha sıklıkla HTTP'nin GET ve POST metotlarını kullanırlar, aşağıda ise HEAD metodu kullanılarak gerçekleştirilmiş örnek bir bağlantı yer almaktadır.

```
[root@       ~]# telnet www.[redacted].edu.tr 80

Trying 80.251.[redacted]...
Connected to www.[redacted].edu.tr (80.251.[redacted]).
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 302 Found
Date: Fri, 17 Oct 2014 06:09:39 GMT
Server: Apache/2.2.15 (Red Hat)
X-Powered-By: PHP/5.3.3
Location: http://[redacted].edu.tr/wp-signup.php?new=
Cache-Control: max-age=0
Expires: Fri, 17 Oct 2014 06:09:39 GMT
Vary: Accept-Encoding,User-Agent
Connection: close
Content-Type: text/html; charset=UTF-8

Connection closed by foreign host.
```

Şekil 3. HEAD Metoduyla HTTP Parmak izi Tarama

HTTP parmak izi tarama işlemini otomatik hale getiren ve farklı yöntemlerle daha detaylı sonuçlar elde edebilen httprint, httprecon, httsquash, whatweb gibi bazı yazılımlar mevcuttur.

Bu çalışmada "httprint v0.301" yazılımı kullanılmış olup sunucunun gönderdiği başlık bilgisinin doğru ve yeterli olduğu kabul edilmiştir (Banner Reported).



Şekil 4. httprint Tarama Sonucu

httprint programı ile yapılan HTTP parmak izi tarama sonucunda elde edilen bilgilere göre Apache, IIS, nginx, lighttpd, vb. biçimde sunucuların türünün ve sürümünün tespit edilebildiği görülmüştür. Ayrıca daha düşük bir oranda da olsa İşletim Sistemi türünün Windows, Unix/Linux, BSD, vb. olarak tespit edilebildiği görülmektedir.

Özellik	✓	✗	Tespit Başarı Oranı
Sunucu Türü	189	7	96.43%
Sunucu Yazılım Sürümü	157	39	80.10%
İşletim Sistemi Türü	149	47	76.02%

Tablo 1. httprint Parmak izi Tarama Tespit Sonucu

Bu çalışmada başlık kısmındaki belirli parametreler incelenmiştir, dönen cevapta varsayılan olarak yer almasa da bazı sunucular tarafından gönderilen alternatif bilgilerle işletim sistemi tespit oranını daha da artırmak mümkündür. Örneğin aşağıdaki sunucu cevabındaki "X-Powered-By" parametresinden sunucunun Ubuntu Linux işletim sistemine sahip olduğu kolaylıkla anlaşılmaktadır.

```
Content-Encoding gzip
Content-Language tr
Content-Type text/html; charset=utf-8
Date Fri, 17 Oct 2014 12:01:55 GMT
Etag "1413545192-0"
Expires Sun, 19 Nov 1978 05:00:00 GMT
Keep-Alive timeout=5, max=100
Last-Modified Fri, 17 Oct 2014 11:26:32 +0000
Set-Cookie TS01fccf47=01eb36f731c9241bf1f129d4ac007
; Path=/
Transfer-Encoding chunked
Vary Cookie,Accept-Encoding
X-Drupal-Cache HIT
X-Generator Drupal 7 (http://drupal.org)
X-Powered-By PHP/5.3.10-1ubuntu3.13
```

Şekil 5. HTTP Parmak izi Taraması Sonucu Elde Edilen Başlık Bilgisi

HTTP parmak izi taraması sonucu başlık kısmındaki belirli parametreler incelenerek elde edilen bilgilere göre üniversitelerin ana sayfalarını barındıran sunucularda kullanılan işletim sistemi ve sunucu yazılım türü dağılımı aşağıdaki gibidir.

İşletim Sistemi Türü	Üniversite Sayısı	Kullanım Oranı
Belirlenemeyen	47	23,98%
Microsoft Windows	90	45,92%
Unix/Linux/BSD	59	30,10%

Tablo 2. Üniversitelerin ana sayfalarını barındıran sunucularda kullanılan işletim sistemi türü dağılımı

Web Sunucu Türü	Üniversite Sayısı	Kullanım Oranı
Belirlenemeyen	7	3,57%
Apache	92	46,94%
LiteSpeed	1	0,51%
Microsoft-IIS	87	44,39%
nginx	9	4,59%

Tablo 3. Üniversitelerin ana sayfalarını barındıran sunucularda kullanılan sunucu yazılım türü dağılımı

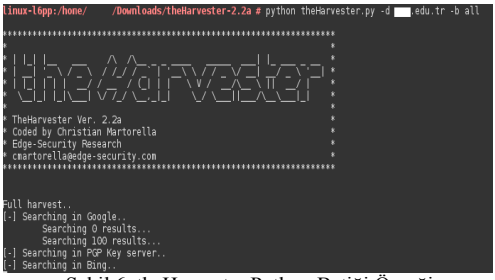
Tespit edilen sunucu yazılım sürümlerine dair www.cvedetails.com, www.osvdb.org nvd.nist.gov, www.kb.cert.org/vuls/ gibi zafiyet veri tabanlarında arama yapıldığında yaması yüklenmemiş sürümlere ait istismar edilebilecek zafiyetlerin olduğu görülmüştür.

3.2. E-posta Hasadı (E-mail Harvesting)

E-posta hasadı çok sayıda e-posta adresinin farklı metotlarla toplu olarak elde edilmesi işlemidir. E-posta hasadı sonucunda elde edilen e-posta adresleri toplu (bulk) e-posta gönderimi, istenmeyen e-posta (spam) gönderimi, oltalama (phising) ve sosyal mühendislik (social engineering) amacıyla kullanılabilmektedir.

E-posta hasadı aşağıda örnekleri belirtildiği üzere birçok farklı kaynak ve teknik kullanılarak gerçekleştirilebilmektedir:

- Web sayfalarından,
- E-posta listelerinden,
- Farklı doküman ve Web formlarından,
- İnternet sohbet odalarından,
- Finger sorgulamalarından,
- Alan adı kayıt ve iletişim bilgilerinden,
- Farklı metotlarla tahmini deneme sonuçlarından,
- Sosyal mühendislik yöntemleri kullanılarak elde edilen sonuçlardan,
- Web sayfalarını ele geçirmek suretiyle elde edilen verilerden,

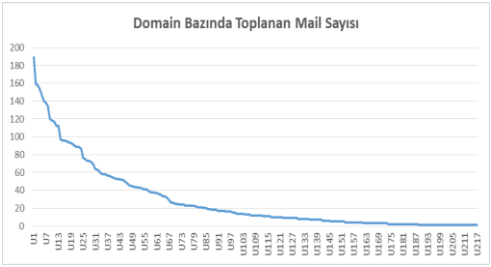


Şekil 6. theHarvester Python Betiği Örneği

Bu çalışmada, kamuya açık web kaynaklarından e-posta hasadı yapmak için kullanılabilecek yazılımlardan biri olan Python dilinde yazılmış "theHarvester 2.2a" [7] betiği kullanılmıştır.

Betik, Google, Google kullanıcı profilleri (Google-profiles), Bing, PGP sunucuları, Linkedin, Shodan gibi farklı arama motorlarından ve sosyal paylaşım sitelerinden 217 farklı domainde toplam 6.236 tekil e-posta adresi toplayabilmiştir. Yapılan çalışmada YÖK veri tabanında kayıtlı olmayan 21 farklı domain tespit edilmiş olup bunların bazılarının veri tabanında yer almayan farklı üniversiteler, bazılarının ise veri tabanında kayıtlı üniversitelerin farklı biçimde yazılan domainleri olduğu görülmüştür. Kayıtlı domainlerden farklı biçimlerde de olsa tamamına ait en az bir adet e-postanın kamuya açık kaynaklar üzerinden erişilebilir olduğu görülmektedir. Ayrıca arama motorlarının sıralaması, bot olarak algılaması ve erişilen web sayfaların anlık

durumu değişebildiğinden betiğin çıktısı ve tespit edilen e-posta sayısı da farklı zamanlarda farklılık gösterebilmektedir.



Şekil 7. E-posta hasası sonucu üniversite – tespit edilen e-posta sayısı grafiği (Maks:189, Min:1)

Tespit edilen e-posta adresleri incelendiğinde *adınilkharfi.soyad@domain, ad.soyad@domain, adsoyad@domain, ogrencino@domain* gibi saldırganlar tarafından kolaylıkla tahmin edilebilir biçimlere sahip olduğu görülmektedir. Her ne kadar işletme açısından kolaylık sağlasa da bu yapısal uygulama zafiyeti e-posta sistemlerinin sözlük atağı gibi saldırılara açık olmasına sebep olmaktadır.

Çalışmada elde edilen sonuç, üniversite domainlerine ait e-posta adreslerinin kamuya açık ortamlardan kolaylıkla toplanabileceği ve bunların siber saldırılar esnasında kullanılabileceği şeklindedir. E-posta adreslerinin kullanımında bilgi güvenliği farkındalığını artırılması ve temel önlemlerin alınması siber güvenlik ile ilgili risklerin azaltılmasına katkıda bulunacaktır.

4. Sonuç ve Öneriler

HTTP parmak izi taramalarını önlemek ve genel anlamda siber güvenliği sağlamak adına atılması gereken ilk adım sunucunun/ hizmetin internet veya intranet üzerinden genel kullanıma açılmadan önce ilgili sunucuda hem işletim sistemi hem de web sunucu yazılımı için sıkılaştırma (hardening) işlemleri ve güvenlik denetimlerinin (sızma testlerinin) yapılmasıdır.

Örneğin; Apache Web sunucunun sıkılaştırılması esnasında aşağıdaki yapılandırmanın kullanılması, sunucu ve işletim sistemi hakkında bilgi toplanmasını önleyecektir.

 # vim /etc/httpd/conf/httpd.conf (RHEL/CentOS/Fedora)
 # vim /etc/apache/apache2.conf (Debian/Ubuntu)

ServiceSignature Off
ServerTokens Prod

 # service httpd restart (RHEL/CentOS/Fedora)
 # service apache2 restart (Debian/Ubuntu)

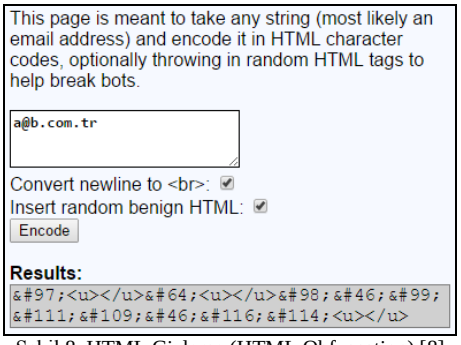
Bu örnek dışında dizin listelemenin engellenmesi, işletim sistemi ve web sunucu yazılımının güvenlik yamalarının takip edilerek zamanında güncellenmesi, gereksiz web sunucu modüllerinin devre dışı bırakılması, kullanıcı ve grupların okuma/ yazma/erişim izinlerinin olması gerektiği şekilde düzenlenmesi, hassas bilgi içeren web sayfalarının kullanıcı adı/şifre ile korunması, Apache web sunucuda "mod_security" ve "mod_evasive" gibi güvenlik modülerinin, IIS web sunucuda "urlscan" gibi ISAPI (Internet Server Application Programming Interface) filtrelerinin kullanılması, web sunucuya yapılacak istekler için limitleme yapılması, SSL sertifika kullanımı ve web sunucuda loglamanın aktif edilmesi, vb. sıkılaştırma ve siber güvenlik ile ilgili yapılabilecek diğer işlemlerdir. Çalışmada tespit yüzdeleri dikkate alınarak Apache ve ISS sunucu türlerine değinilmiş olup diğerleri için de kendilerine özgü benzer sıkılaştırma işlemlerinin yapılması elzemdir. Web sunucu sıkılaştırma için ortak katılımla daha kapsamlı, detaylı güvenlik kontrol listelerinin / kılavuzlarının hazırlanması, paylaşılması ve sürekli olarak güncellenmesi faydalı olabilir.

Farklı kaynaklardan çeşitli teknikler kullanılarak gerçekleştirilebilecek E-posta hasadına ve olumsuz sonuçlarına maruz kalmamak adına aşağıda belirtilen yöntemler kullanılabilir.

- E-posta adres biçimini "@" işareti yerine "[at]", "." yerine de "[nokta]"

yazarak sıradan kullanıcıların anlayabileceği şekilde değiştirmek,

- E-posta adresini metin yerine resim biçimine dönüştürerek kullanmak,
- İletişim için E-posta adresi yerine iletişim formu kullanmak,
- JavaScript gibi bir betik dili kullanarak e-posta adreslerini farklı algoritmalar ile kodlayarak gizlemek,
- E-posta adreslerini HTML karakter kod ve etiketleri kullanarak gizlemek,



Şekil 8. HTML Gizleme (HTML Obfuscation) [8]

- E-posta hasadı yapan robot yazılımları (bot), CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) kullanarak bertaraf etmek,
- E-posta hasadı amacıyla web sayfasını tarayan robot yazılımlardan (web spider/crawler) kaçınmak için tuzak web sayfaları (spider trap) kullanmak.
- Siber güvenlik farkındalığını arttırarak kullanıcıların e-posta adreslerini genele açık, güvensiz ortamlarda kullanmamalarını sağlamak,
- E-posta sunucularında varsayılan ayarların değiştirilerek (TCP port numaralarını değiştirmek, SSL kullanımını zorunlu kılmak vb.) e-posta hasadı gibi vakalara karşı dayanıklı hale getirilmesini sağlamak (hardening),

Web sitelerinde "robots.txt" gibi bir dosya kullanarak "* Disallow <dizin_adı>" komutuyla dizinlerin taranmasını engellemeye çalışmak aslında gerçek hedeflerin açık edilmesi anlamına gelmektedir, böyle bir yöntemi kullanmanın günümüzde anlamsız kaldığı söylenebilir. Zira web sayfası, <meta name="robots" content="noindex,nofollow"> HTML etiketiyle Google botlarından korunmaya çalışılsa bile Google, taramasını mutlaka gerçekleştirmekte ve söz konusu siteyi indekslemektedir.

Ayrıca bu iki yöntemle keşif yapılmasını önlemek amacıyla;

- Saldırı Tespit ve Önleme Sistemleri (IDS/IPS), Güvenlik Duvarı (Firewall), İçerik Filtreleme (Content Filtering), AntiVirüs/AntiSpam gibi ağ geçidi (gateway) şeklinde konumlandırılabilen güvenlik cihazlarının/ürünlerinin doğru şekilde yapılandırılarak kullanılması,
- Periyodik güvenlik denetimlerinin (penetration testing and auditing) yapılması,
- Sistem loglarının sürekli ve sistematik şekilde gözlenmesi (log monitoring and analysis) de siber güvenliğin sağlanmasında katkı sağlayacaktır.

Siber Güvenlik konusunda en zayıf halka insan olduğundan alınması gereken ilk ve en önemli önlem, idari yöneticiler, sistem yöneticileri ve son kullanıcılar gibi tüm seviyedeki kullanıcıların bilgi güvenliği farkındalığının oluşturulmasıdır.

Kaynaklar

[1] Resmi Gazete: http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

[2] http://www.securitysift.com/passive-reconnaissance/

[3] http://www.zone-h.org/archive/filter=1/domain=edu.tr/fulltext=1/page=1

[4] http://www.yok.gov.tr/web/guest/universitelerimiz

[5] http://www.wikiwand.com/en/Device_fingerprint

[6] Karaarslan, E., Tuglular, T., Sengonca, H., 'Does Network Awareness Make Difference in Intrusion Detection of Web Attacks', ICHIT 2006

[7] http://code.google.com/p/theharvester/

[8] http://isnoop.net/tools/obfuscate.php