Istanbul Commerce University Journal of Science
İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 16(31), Bahar 2017
http://dergipark.gov.tr/ticaretfbd

Tarama Makale

VERİ VE AĞ GÜVENLİĞİ İÇİN UYGULAMA VE ANALİZ ÇALIŞMALARI*

Ömer Faruk KAYA[1] **Erdinç Öztürk**[2]

[1] İstanbul Ticaret Üniversitesi, Siber Güvenlik Yüksek Lisans Programı, İstanbul, Türkiye
omfaka@gmail.com
orcid.org/0000-0002-0851-0617

[2] İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, İstanbul, Türkiye
eozturk@ticaret.edu.tr
orcid.org/0000-0003-1553-2619

Öz

Günümüzde artık bir yaşam biçimi halini alan bilgisayar dünyasında dosyaları, bilgileri özetle veriyi korumak en önemli konu olarak karşımıza çıkmaktadır. Özellikle paylaşımlı ve halka açık iletişim sistemlerinde veri güvenliği daha da fazla önem arz etmektedir. Bir diğer önemli konu ise ağ güvenliğidir ki son kullanıcı ve merkez arası haberleşme protokolleri ile sağlanan haberleşme yöntemlerinde veriyi korumak hayati önem taşır. Ağ güvenliği tedbirleri verinin iletimi sırasında onun korunmasını esas alır. Bu çalışmada özellikle 150'ye yakın saha lokasyonu olan bir kamu kuruluşunda saha ile merkez arası network ve veri güvenliği ile merkezde bu alanda alınması gereken önlemlerin vurgulanması hedeflenmiştir. Ayrıca, İstanbulkart'ın İspark uygulamalarına entegrasyonu sırasında bu önlemlerin uygulanması ile ortaya çıkan güçlükler ve sonuçlar bu çalışma ile sunulmuştur.

Anahtar Kelimeler: *Siber Güvenlik, Ağ güvenliği, Veri Güvenliği.*

Review Article

APPLICATION AND ANALYSIS STUDIES FOR DATA AND NETWORK SECURITY

Abstract

As the digital world emerges as a new lifestye, protecting private data in this world turns out to be a very important topic. Especially for shared and public systems, data security poses much higher importance. Another important topic is network security and it is crucial to protect the data in communication between end user and the server via secure communication protocols. Network security measures are based on protecting the data during its communication. In this work, we emphasize the necessary precautions that is required for network and data security for a public institution that has more than 150 field locations. Furthermore, the challenges and results that ocurred during İspark integration of İstanbulkart is presented in this work.

Keywords: Cyber Security, Network Security, Data Security.

* Received / Geliş tarihi: 08/02/2017 Accepted / Kabul tarihi: 20/06/2017
[1] Corresponding Author/ Sorumlu Yazar : omfaka@gmail.com

1. GİRİŞ

Veri ve ağ güvenliği demek, bütün işyerleri, kamu ve üniversiteler dahil veri haberleşmelerini birbirine bağlı ağlar üzerinden yaptıklarından ortaya ortak bir ağın çıkmasıyla birbirine bağlı ağlar kavramı da ortaya çıkmaktadır. Bu durumda koruma, ağdaki bütün birimleri kapsar. Bilgiye ulaşımı sağlayan hizmetler (http,ftp,vb.) aynı zamanda zararlı hale gelebilir. Burada yapılması gereken zararı minimize etmektir. Dolayısıyla veri ve ağ güvenliğinde atılacak her bir adım için öncelikle korunması gereken varlıkların tespit edilmesi gerekmektedir.

1.1 Korunması Gereken Varlıklar

Bu bölümde veri güvenliğinin sağlanması için gereken varlıklar ele alınmaktadır.

1.1.1 Veriler

Verilerin güvenliği üç maddede özetlenebilir;

- **Gizlilik:** Verilerin başkaları tarafından görüntülenmesinin istenilmemesi,
- **Bütünlük:** Verilerin başkaları tarafından değiştirilmesi istenilmemesi,
- **Erişilebilirlik:** Verilerin istenildiği zaman ve mekandan ulaşılabilir ve kullanıma hazır olmasının istenmesi.

1.1.2 Kaynaklar

Kurum içindeki bilgisayarlardaki kaynaklara (hard disk, işlemci, bellek vb.) ulaşımın tamamen kısıtlanması gerekir. Aksi düşünülemez. Bunun sebebi erişim halinde öngörülemeyen boyutlarda güvenlik riskleri oluşturmasıdır.

1.1.3 Saygınlık

Kurumun saygınlığının gerçek hayatta olduğu gibi sanal ağ üzerinden de korunması gerekir. Herhangi bir veri sızıntısı veya hacking olayında kurumun karşılaşacağı itibar kaybı telafisi mümkün olmayan sonuçlar doğurabileceği gibi kurumun güvenliğini de derinden sarsacak bir durum oluşturur.

2. TEMEL BİLGİLER

Çalışmada, önceki başlıklarda bahsi geçen varlıkların korunması adına öncelikle bir güvenlik politikası oluşturmak ve geliştirmek zaruridir. En iyi güvenlik, kurumdaki merkez ve saha haberleşmelerini sağlayan ağ tasarımının sağlamlığı ve kişilerin erişilebilirlik yetkilerinin sınırlanması ile başlar. Kurumdaki güvenlik politikası güvenliğin en temel öğesidir. Bu politika ile korunmasına önem verilen veriler/varlıklar belirlenir. Bunu belirlemek adına öncelikle, hangi personelin nerde, ne zaman ve ne tür bir yetki ile donatılacağı soruları sorulmalıdır. Bu politika olabildiği kadar sade ve diğer çalışanlar tarafından anlaşılabilir olmalıdır.

Politikanın hazırlanıp kurum içi bilgilendirme yapıldıktan sonra yapılması gereken, kurulan networkü ve fiziksel cihazları (sunucular, modem, router, switchler vb.) iç

ve dış tehditlere karşı korumak olmalıdır. Bunun için de öncelikle varlıklarımıza karşı gelebilecek risklerin analizi yapılmalıdır.

3. RİSK ANALİZİ

Risk analizi korunacak varlıklarımızın ve potansiyel saldırıların belirlendiği süreçtir. Doğru risk analizinin yapılması önemli bir maddedir. Bu analizi sağlıklı yapabilmek adına bazı sorular sorulmalıdır.

- Korunacak varlıklar nelerdir?
- Varlıklarımızı nelerden korumalıyız?
- Gelecek bir zararda kuruma maliyeti ne olacaktır?
- Kimler saldırı düzenleyebilir?
- Yapılan saldırı sonucunda varlığımızın veya verinin bozulma/kaybolma olasılığı nedir?
- Kaybolan verinin geri yüklenmesi için harcanan maliyet ne olacaktır (Yedekleme Maliyeti)?

Bu gibi sorular veri ve ağ güvenliğinin sağlanmasında en önemli aşamayı oluşturmaktadır.

Bu çalışmada, üstte sayılan tüm yöntemler uygulandıktan sonra kurum için kullanılan çeşitli metod ve yöntemlerle penetrasyon testleri ve sonuçları üzerinde bir çıkarım yapılmıştır. Öncelikle penetrasyon testi kavramı ve zafiyet tarama ile ilgili bilgi verildikten sonra bu çıkarımlar üzerinde bulunan açıkların raporlamasını yaparak açıkların kapatılması adına neler yapılması gerektiği gösterilecektir.

4. UYGULAMA

Bu bölümde penetrasyon testi çeşitleri ve özellikleri açıklanmıştır. Devamında uygulama ile ilgili bilgilere yer verilmiştir. Sonuç bölümde ise uygulama değerlendirmeleri ve sonuçlar tartışılmıştır.

4.1 Penetrasyon Testi

Temel olarak belirli güvenlik düzeyindeki ihlallerin bulunması ve ardından bu ihlallerin azaltılması, gereken adımların atılmasını sağlamak için var olan güvenlik mekanizmalarını denetleme ve bu mekanizmaları atlatma denemelerinden oluşur.

Veri ağları ve sistemlere saldıran kişilerin sayısı, bilgi ve becerisi, zamanı ve motivasyonu her zaman güvenlik uzmanlarının sahip olduğu zaman, bilgi ve motivasyonun üstündedir. Bilişim güvenliği temelde ikiye ayrılırsa bunun biri savunmacı güvenlik olarak adlandırılan korumacı güvenlik, diğeri de proaktif güvenliktir. Penetrasyon testi çalışmaları proaktif güvenlik anlayışının bir sonucudur.

4.2 Test Süreçleri

Penetrasyon testinin yapılması birkaç aşamadan oluşur. Bu test sayesinde dışarıdan saldırgan bakış açısıyla güvenlik açıklarının kontrolü ve raporlanması sağlanır. Sistemlerin kendi içlerindeki güvenlik tedbirleri çoğunlukla yeterli olmamakta ve önlemler güncelliğini koruyamamaktadır. Ayrıca kötü niyetli kişilerin sayısının artması ve bilgi düzeylerinin genellikle bir çok şirket çalışanından önde olması pentestin önemini ortaya koymaktadır. Pentest bir şirketin bilişim sistemleri için iç ve dış tehditlere karşı güncel önlemler alınmasını ve zafiyetlerin giderilmesini sağlar. Bu sayede;

- Saldırılara karşı daha dirençli bir bilişim altyapısı oluşturulur.
- Kullanıcı bazlı olarak bilgi güvenliği farkındalığı artar.
- Sistemlerin durdurulma veya kaynak doldurmalar engellenir.
- Kurum prestijinin ve marka değerinin korunması sağlanır.

Bu test süreci veri ve ağ güvenliğinin altyapısını oluşturur. Aşağıda test bileşenleri ve kullanılan temel elemanlar açıklanmıştır.

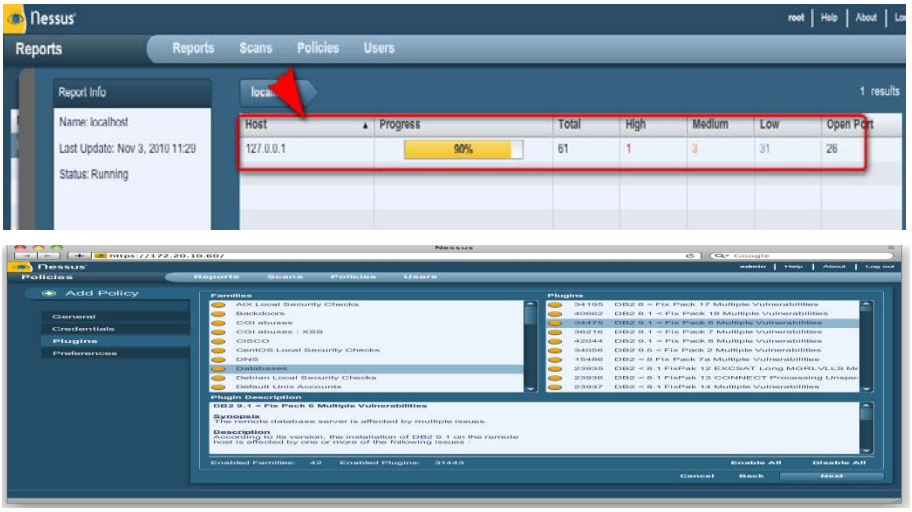
4.2.1 Zafiyet Tarama Süreci ve Kullanılan Temel Araçlar

Bu sürecin amacı belirlenen hedef sistemlerdeki açıklıkların ortaya çıkarılmasıdır. Bunun için sunucu servislerdeki bannerler ilk aşamada kullanılabilir. Ek olarak birden fazla zayıflık tarama aracı ile bu sistemler ayrı ayrı taranarak oluşabilecek false positive oranı düşürülmeye çalışılır.

Bu aşamada hedef sisteme zarar vermeyecek taramalar gerçekleştirilir. Zayıflık tarama sonuçları mutlaka uzman gözler tarafından tekrar tekrar incelenmeli, olduğu gibi rapora yazılmamalıdır. Otomatize zafiyet tarama araçlar ön tanımlı ayarlarıyla farklı portlarda çalışan servisleri tam olarak belirleyememektedir.

4.2.1.1 NESSUS

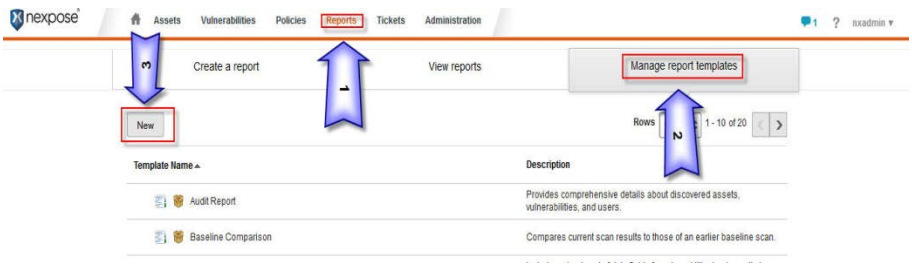
Güvenlik camiasının ilk açık kod zafiyet tarayıcılarındandır (bkz. Şekil 1). 3.x sürümüyle birlikte lisans modeli değişmiştir. Ücretsiz olarak ticari amaç harici kullanılabilir. Piyasadaki en iyi açıklık tarayıcılardandır. Kendi açıklık tanımlama dili (NASL) sahiptir. Ashe (2004) , NESSUS kullanarak yapılan bir örnek çalışmayı anlatmaktadır.



Şekil 1. Nessus

4.2.1.2 NEXPOSE

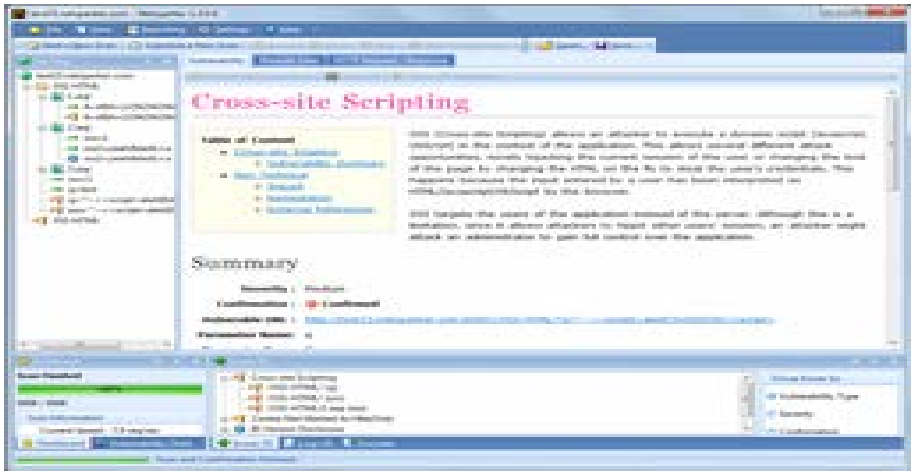
Rapid7 için çalışan Nexpose tüm güvenlik açığı yönetimi yaşam döngüsünü desteklemeyi amaçlayan bir güvenlik tarayıcısıdır (bkz. Şekil 2). Keşif, tespit, doğrulama, risk sınıflandırması, etki analizi, raporlama ve hafifletme bölümlerini içerir (Soğukpınar (2010)).



Şekil 2. Nexpose

4.2.1.3 NETSPARKER

Netsparker tespit ve güvenlik açılarından yararlanmayı da içeren bir web uygulama güvenliği tarayıcısıdır (bkz. Şekil 3). Başarılı bir istismar sonrası teyit edilen açıklıkları raporlar aksi halde bulduğunu test eder. Netsparker web sitesinde bu araç detaylı olarak anlatılmaktadır.



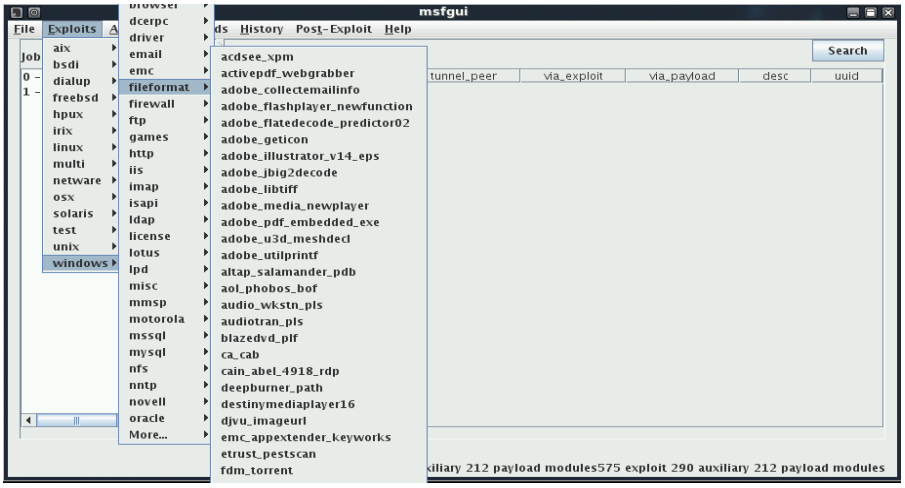
Şekil 3: Netsparker

4.2.2 Sızma Süreci ve Kullanılan Temel Araçlar

Belirlenen açıklıklar için POC kodları/araçları belirlenerek denemeler başlatılır. Açıklık için uygun araç yoksa ve imkan varsa ve test için yeteri kadar zaman verilmişse sıfırdan yazılır. Genellikle bu tip araçların yazımı için Python, Ruby gibi betik dilleri tercih edilir. Bu adımda dikkat edilmesi gereken en önemli husus çalıştırılacak exploitlerden önce mutlaka yazılı onay alınması ve mümkünse laboratuvar ortamlarında önceden denenmesidir.

4.2.2.1 METASPLOIT

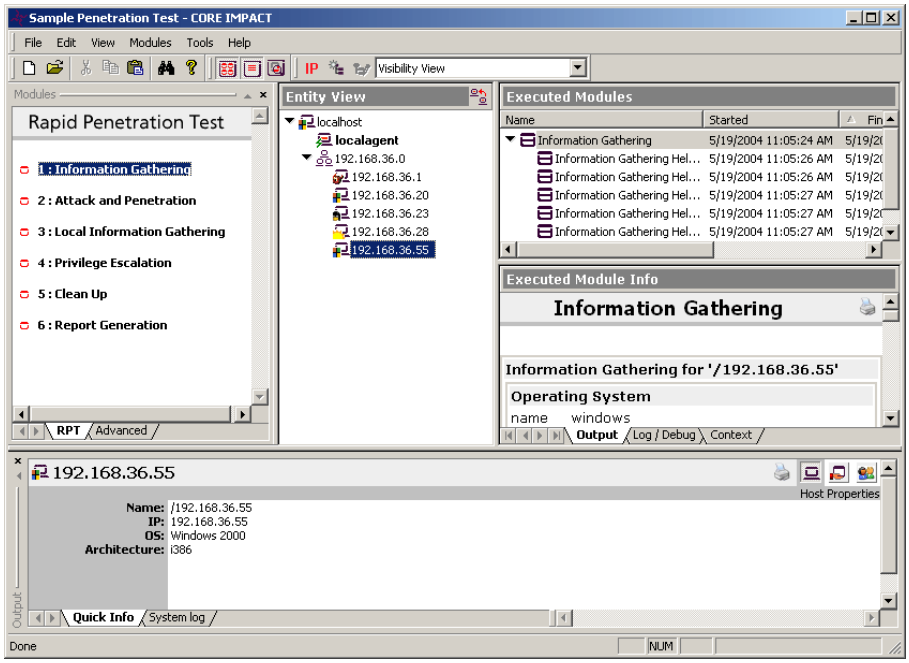
Açık kaynak kodlu exploit geliştirme ve çalıştırma aracı. 600~ civarı çalışan exploit barındırır (bkz. Şekil 4). Aux modülleriyle bilgi toplama, ağ keşfi gibi işlemler gerçekleştirilebilir. Web, GUI ve konsoldan çalıştırılabilir. Gelişmiş AV, IPS atlatma özelliklerine sahiptir. Bir güvenlikçinin mutlaka kullanması gereken araçların başında gelir. Rapid7 firması tarafından satın alınmıştır.



Şekil 4: Metasploit

4.2.2.2 CORE IMPACT

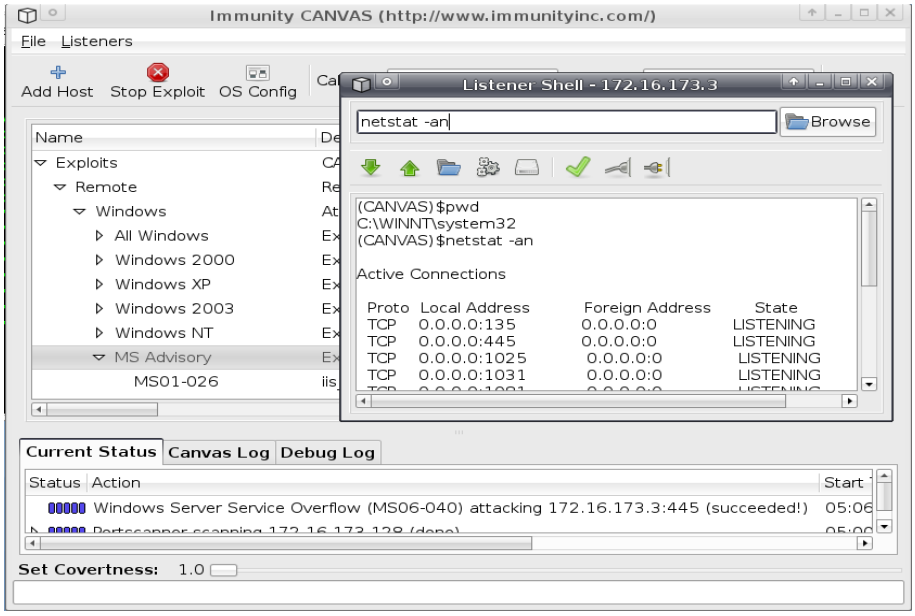
Pahalı olmasına rağmen yaygın olarak kullanılan en güçlü işleme aracı olarak kabul edilir (bkz. Şekil 5). Düzenli güncellenen veritabanı sayesinde profesyonel exploitler yaparak diğer makinalara kurduğu tünel sayesinde onları rahatlıkla exploit edebilir (Soğukpınar (2010)).



Şekil 5: Core Impact

4.2.2.3 IMMUNITY CANVAS

Ticari bir tool'dur. 370'den fazla exploit içerir. Core Impact ve Metasploit'in ücretli sürümünden daha ucuzdur. Full kaynak kodu ile ve bazen de zero day açıklık bilgileri ile gelir (bkz. Şekil 6). Önal (2010) da yazar bu araç hakkında detaylı bilgi vermektedir.



Şekil 6: Immunity Canvas

4.2.2.4 SQLMAP

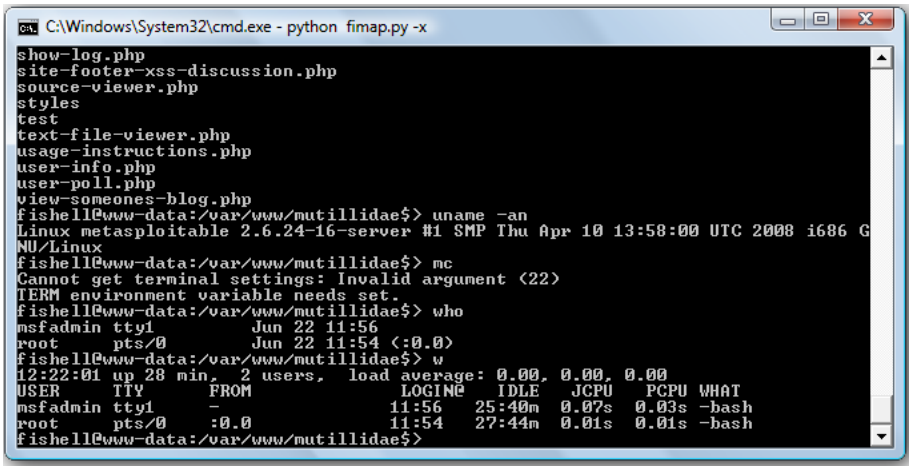
SQL injection'ları tespit eden ve kusurları istismar ederek arak uç Veritabanı sunucularına erişimi sağlayan açık kaynaklı penetrasyon aracıdır (bkz. Şekil 7). Out of band yoluyla işletim komutları DB'den veri getiriyor hatta temel dosya sistemine erişim sağlıyor (Soğukpınar (2010)).

Şekil 7: SqlMap

4.2.2.5 FIMAP

Fimap bir python aracıdır. Bu araç, bulur, hazırlar, denetimi yapar, istismar eder ve webapps'lerdeki bug'ları bulur (bkz. Şekil 8). Sqlmap'e benzer, farkı LFI / RFI bugları bulmasıdır.

Önal (2010) da yazar bu araç hakkında detaylı bilgi vermektedir.



Şekil 8: FIMAP

4.2.3 Şifre Kırma Süreci ve Kullanılan Temel Araçlar

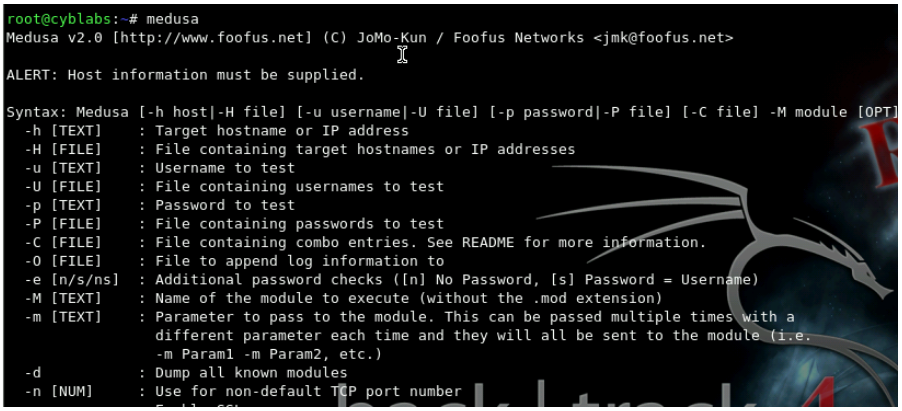
Şifre ve parolalar siber dünyanın en zayıf halkalarından biridir. Tek bir parola tüm güvenlik sistemlerini devre dışı bırakarak sistemin ele geçirilmesine sebep olabilir. Parola(şifre) kırma yöntemleri

- Online parola(şifre) kırma (Aktif)
- Offline parola(şifre) kırma (Pasif)

Aşağıda şifre kırma sürecinde kullanılan yöntemlerle ilgili bilgiler verilmiştir.

4.2.3.1 MEDUSA

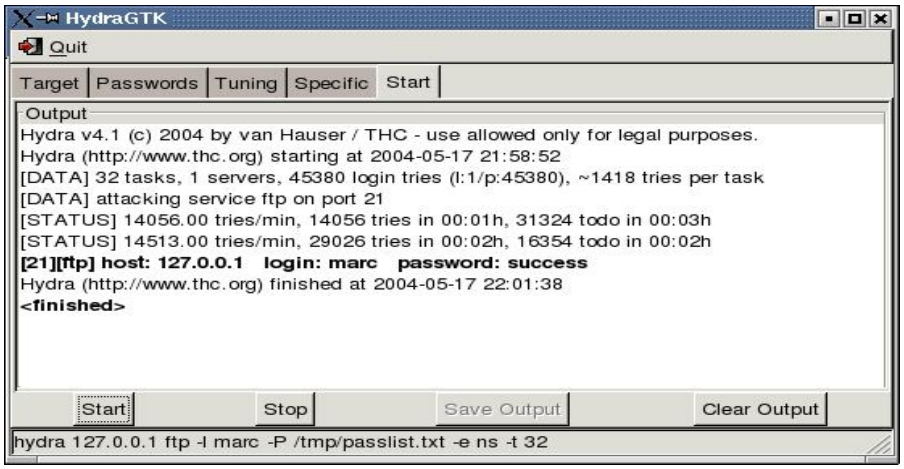
Ağ üzerindeki servislere yönelik (http, telnet, ssh, ftp gibi) aktif parola kırma aracıdır (bkz. Şekil 9). Farklı portlarda çalışan servisler için port ayarı yapılabilir. Paralel saldırı düzenleme seçeneği vardır. Ağ bağlantısına ve servisin durumuna göre hızı değişmektedir.



Şekil 9: Medusa

4.2.3.2 HYDRA

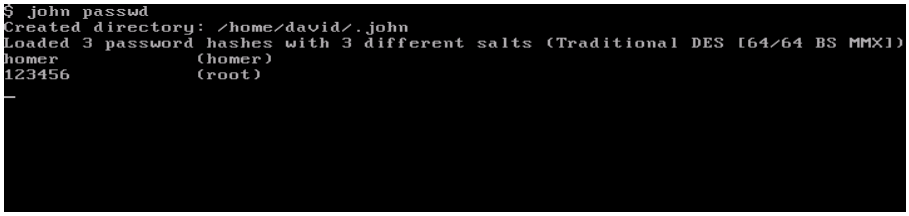
Paralel ağ servisleri parola denetim(kırma) aracıdır (bkz. Şekil 10). Konsol ve grafik arabirimden çalıştırılabilir. Hesap kitleme riski vardır. 30'dan fazla protokole karşı (telnet, ftp, http, https, smb vb.) brute force ataklarda kullanılır.



Şekil 10: Hydra

4.2.3.3 JOHN THE RIPPER

Pasif şifre kırma(denetim) aracıdır (bkz. Şekil 11). Bilgi toplama vs sonrası ele geçirilen hashlenmiş parola dosyalarını kırmak için kullanılır. Yeni nesil Linux parolaları (Sha512 kullanılmış) JTR kırmak için ufak bir yama gerekir (Soğukpınar (2010)).



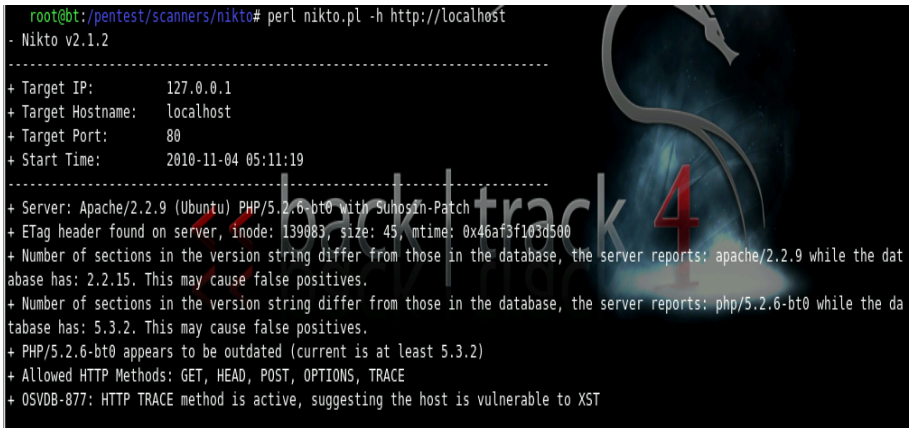
Şekil 11: John The Ripper

4.2.4 Web Uygulama Güvenlik Testleri ve Kullanılan Temel Araçlar

Siber dünyanın yeni gözdesi web uygulamalarıdır. Her yazılan kod ayrı bir güvenlik riski oluşturur. Henüz oturmuş bir yazılım geliştirme standardının olmaması sebebiyle çeşitli güvenlik açıklıkları bulunmaktadır. Gartner'a göre zafiyetlerin %75'i web uygulamalarında, güvenlik için harcanan paranın %90 ağ güvenliği üzerine olmaktadır.

4.2.4.1 NIKTO

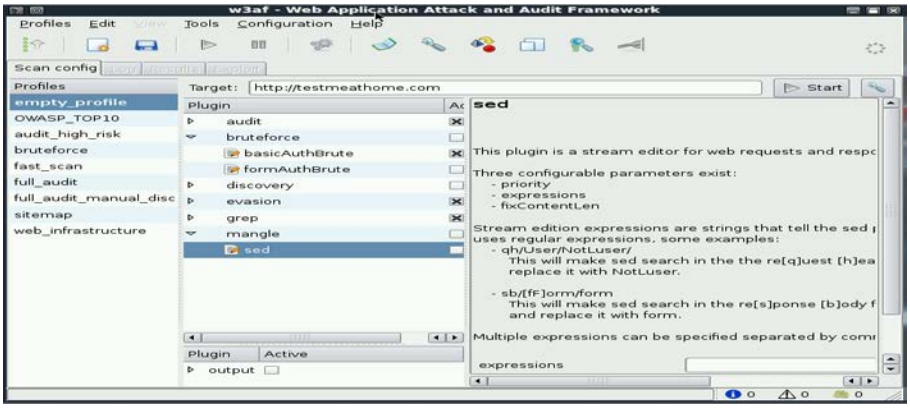
Statik web açıklık tarayıcısıdır (bkz. Şekil 12). Aynı zamanda ilk web açıklık tarayıcılarındandır. Güvenlik açıklığı barındıran web sunucu yazılımları, test, dev. gibi yanlışlıkla unutulmuş dosyaları, yapılandırma hatalarını bulmak için kullanılır. Nessus entegrasyonu vardır. Günümüz uygulamaları için yeterli değildir (Soğukpınar (2010)).



Şekil 12: Nikto

4.2.4.2 W3AF

Web aplikasyonu açıklıklarını bulmada son derece popüler, güçlü ve esnek bir araçtır (bkz. Şekil 13). Kullanımı kolay bir ara yüze sahiptir. Birçok web değerlendirme özellikleriyle istismar eklentilerinin gelişiminde kullanılmaktadır.



Şekil 13: W3AF

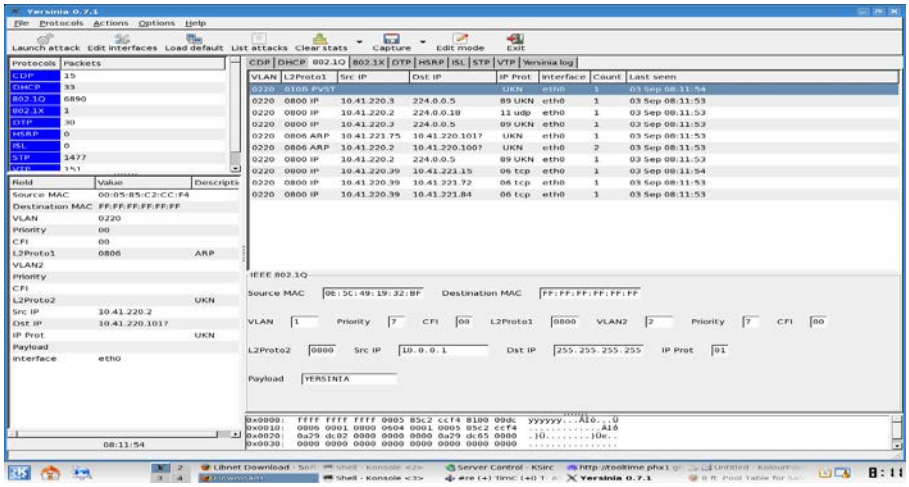
4.2.5 Yerel Ağ Protokolleri Güvenlik Testleri Süreci ve Kullanılan Temel Araçlar

Yerel ağ protokolleri güvenlik testleri genellikle önemsenmez ya da ikinci plana atılır. Yerel ağ saldırılarını sağlıklı olarak test edecek yazılım eksikliği "Yersinia" ile sık kullanılan LAN protokollerini test amaçlı "Ettercap" araçları kullanılır.

4.2.5.1 YERSINIA

Bu araç ile birlikte kullanılan protokoller; (bkz. Şekil 14).

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

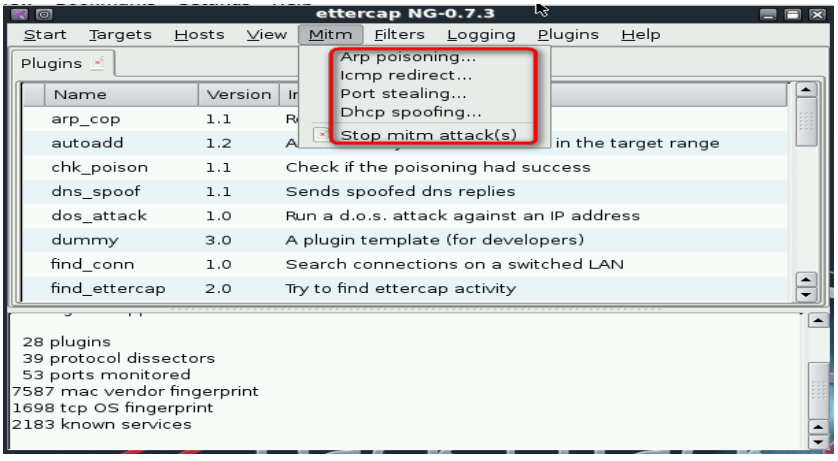


Şekil 14: Yersinia

4.2.5.2 ETTERCAP

Yerel ağlarda araya girme, bilgi çalma ve dos yapmak için kullanılan gelişmiş bir araçtır (bkz. Şekil 15). MITM için çeşitli yöntemler kullanır. Bu yöntemler;

- ARP poisoning
- ICMP Redirect
- Port Stealing
- DHCP spoofing



Şekil 15: Ettercap

4.3 Zafiyet Tespit Araçlarının Artıları/Eksileri

Bu araçlar her zaman kesin sonuç vermezler. Yanıltabilme payları yüksektir. Bulunan her zafiyetin varlığının fiziksel olarak test edilmesi doğru sonuca götürür. Doğru sonuç almak için birden çok araç kullanmak gerekir. Zafiyet tespit etmek için en doğru araç seçilmelidir. Yanlış ürün ile doğru sonuç alınmaz. Hacking evresine yön verir.

4.4 Sonuç/Result

Tüm bu bilgiler ışığında uygulama sonuçları aşağıda tartışılmıştır. Test süreçleri ve ilgili raporlamalar aşağıda yer almaktadır.

4.4.1 Penetrasyon Testi Raporlama Süreci

Penetrasyon testinin ardından yapılacak raporlama sürecinde işlemlerimizi adım adım yaparak öncelikle süreci değerlendirmek en doğru yoldur.

1.Adım: Sistem Güvenliği Ana Hatları

- Ağ düzeyinde proaktif penetrasyon Testi yapılacak tüm aygıtlar listelenir. Sistem güvenliğini sağlayan protokoller, prosesler, ağ bileşenleri, ara birimler ve güvenlik gereksinimleri araştırıldı.

2.Adım: Sistem Zayıflık İncelemesi

- Ağ ve sistemlerde bulunan potansiyel zayıflıklar araştırıldı. 1. Adımda elde edilen bilgiler doğrultusunda potansiyel zayıflık araştırmaları ve saldırı planı geliştirildi. Potansiyel ağ altyapısı zayıflıkları ve eksiklikleri tespit edildi.

3.Adım: Zayıflık Değerlendirmesi

- Ağ haritası çıkarıldı ve 2. Adımdaki tüm bileşenlerde bulunan zayıflıklar değerlendirildi. Hedef analizi sonrası hangi bileşenlere, sistemlere hangi protokollerle saldırılacağı belirlendi.

4.Adım: Araç Analizi

- Araştırma, inceleme ve değerlendirme süreçleri sonrası söz konusu senaryolar için hangi araçların kullanılacağının listesi çıkarıldı.

5.Adım: Penetrasyon Saldırıları

- 4.Adımda belirlenen araçlar ve 3. Adımda belirlenen saldırı senaryosu kullanılarak penetrasyon saldırıları düzenlendi. Bu saldırılar sonucu başarılı olanlar sınıflandırıldı.

6.Adım: Zayıflık Analizi

- Ortaya çıkan zayıflıkların analizi yapılarak ortaya çıkabilecek ek zayıflıklar ve aksiyonlar göz önüne alınarak riskin minimize edilmesi sağlandı. Zayıflıklar arası bağlantılar olup olmadığı risk grubuna göre gözlenir.

7.Adım: Geri Bildirim Süreci

- Sistem güvenlik veritabanı, zayıflık veritabanı ve araçlar düzenlenerek raporlama aşamasına geçildi.

4.4.2 Bulgu Önem Dereceleri

Ağ ve sistemlerde bulunabilecek riskler çeşitli kategorilerde sınıflandırılır. Aşağıda bu risk sınıflandırmalar ve yol açabileceği zararlar ışığında sonuç raporun önem derecesi belirlenir.

Acil Risk Sınıfı

Sistemin bütünlüğünü tehdit eden tarzda saldırılar bu sınıfta görülür. Bu sınıfta bulunan zayıflıklar saldırganın en çabuk şekilde sistemlere erişmesini sağlar. Niteliksiz saldırganlar dahi bu zayıflıklarla sistemlere erişim sağlayabilirler.

Kritik Risk Sınıfı

Bu sınıflandırma sistemde bulunan belli sınıftaki verilere dış ağdan erişim sağlar. Saldırganın sistemleri tamamen ele geçirmesi ile sonuçlanabilecek saldırılara sebep olan açıklıklardır.

Yüksek Risk Sınıfı

Yüksek risk derecesindeki zayıflıklar sistemden bazı kritik bilgi edinme ile sonuçlanabilecek saldırıları tanımlar. Ayrıca yerel ağdan ya da sunucular üzerinden hak yükseltmeyle sonuçlanacak saldırılara sebep olabilirler.

Orta Risk Sınıfı

Yerel ağdan veya sunucu üzerinden gerçekleştirilebilecek, hizmet dışı bırakma, servis engelleme ile sonuçlanan saldırılara sebep olan açıklıklardır.

Düşük Risk Sınıfı

Sistem ile ilgili bilgilerin deşifre edilmesi veya sistem, ağ üzerinde çalışan riskli bir servisin haberdar edilmesi amacıyla kullanılır. Bu sınıfta yer alan sistem ve ağ ile ilgili yöneticilerin haberdar olması için belirtilir. Bu bilgiler ışığında sıkılaştırma (hardening) çalışmaları yapılması gerekir.

5. DEĞERLENDİRME

Son olarak yukarıdaki bilgiler toparlanıp zayıflıklar listelenmiştir (bkz. Şekil 16). Daha sonra da bu zayıflıkların giderilmesi adına çözüm önerileri uygulanmıştır. Sonuç olarak uygulanan çözümün söz konusu zayıflığı ortadan kaldırdığı görülmüştür. Örnek olarak, düşük düzeyde bir zayıflığı ele alacak olursak (bkz. Şekil 16), kullanılan web sunucusunun http başlığı kullanılarak yukarıdaki yöntemlerden uygun olanının kullanılması suretiyle şirket içerisindeki iç IP ifşası mümkün olabilmektedir. Web sunucusu iç ip adreslerini dışarıdaki kullanıcılara ifşa etmektedir. Bu tarz bilgi edinme temelli zayıflıklar saldırganlara iç ağ hakkında bilgi edinme şansı tanımaktadır.

Bu sorunun çözümü olarak yapılması gereken basit bir güncellemenin yeterli olacağı görülmüştür (bkz. Tablo 1). Yama güncellemesi yapıldığı takdirde bu ifşanın önüne geçileceği görülmüştür.

Zayıflık	Bulgu Önem Derecesi
Web Server Dizin Listeme Zayıflığı	Orta
Dışarıya Açık HP Procurve Yönetim Paneli Zayıflığı	Orta
Şifrelenmeden İletilen Web Tabanlı Kimlik Doğrulama Zayıflığı	Orta
Web Otomatik Şifre Tamamlama Zayıflığı	Düşük
Hatalı Tasarlanmış Captcha Kullanımı	Orta
Apache Web Server Çoklu Zayıflıklar	Acil
PHP Çoklu Zayıflıklar	Acil
PHPmyadmin BBcode Tag XSS Zayıflığı	Yüksek
Web Sunucusu HTTP Başlığı İç IP İfşası	Düşük
Dışarıya Açık Kritik Servisler	Orta
Apache Tomcat JSP Varsayılan	Orta

Şekil 16: Zayıflıkların Bulgu Önem Derecesi

Zayıflık	Bulgu Önem Derecesi
VMware ESXi File Descriptors Zayıflığı	Yüksek
VMware ESXi NFC Trafiği Servis Engelleme Zayıflığı	Yüksek
Desteklenmeyen İşletim Sistemi Debian Sarge	Yüksek
Yetkisiz Kritik Dosya Erişimi Zayıflığı	Yüksek
Yapılandırma Sorunu / Zararlı Yazılım / Desteklenmeyen İşletim Sistemi Windows	Acil
MySQL Çoklu Zayıflıklar	Yüksek
ProFTPD Race Condition Zayıflığı	Orta
Nginx Web Server DoS ve Bilgi Edinme Zayıflığı	Yüksek

Şekil 17: Zayıflıkların Bulgu Önem Derecesi

Tablo 1: Web Sunucusu HTTP Başlığı İç IP İfşası

Web Sunucusu HTTP Başlığı İç IP İfşası	
Kullanıcı Profili	Genel Kullanıcı
Erişim Noktası	Kurum Dış Ağı
Önem Derecesi	Düşük
Etkisi	Kurum iç ağı ile ilgili bilgi edinme
Açıklama	Web sunucusu iç ip adreslerini dışarıdaki kullanıcılara ifşa etmektedir. Bu tarz bilgi edinme temelli zayıflıklar saldırganlara iç ağ hakkında bilgi edinme şansı tanımaktadır.
Çözüm	Aşağıda yer alan Microsoft bültenleri yardımıyla sorun çözümlenebilir; http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q218180 http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q834141
Bulgunun tespit edildiği bileşenler	IP/URL: http://…, Port: /tcp…/tcp, Sistem: Windows

6. SONUÇ ve GELECEK ÇALIŞMALAR

Sonuç olarak, yapılan tüm araştırmalar ve testler verinin ve varlıkların korunmasının önemini gözler önüne seriyor. Yapılandırılan kurum ağı, merkez ve saha arasındaki veri iletişiminin sürdürülebilirliği ne kadar önemliyse bu verinin güvenliğini sağlamak da aynı oran da önemlidir. Bu çalışmada ağımızdaki tehditler, önem derecelerine göre farklı araçlarla tespit edilerek çözüm konusunda uygun prosedürler uygulandı ve tehdit bertaraf edildi. Bu çalışma farklı kurumlar için de planlanıyor. Aynı şekilde yapılacak yöntemlerle farklı illerde farklı kurum ve kuruluşlara danışmanlık verilmesi planlanıyor.

Hali hazırda çalışmış olduğum kurumumda (İspark A.Ş.) her yıl düzenli olarak bu testleri yapmaktayız. Özellikle Metasploit ve Coreimpact yöntemlerini kullanarak kullanıcı bilgisayarlarındaki zafiyetlerve sistemde oluşturduğu etkiyi görmüş oluyoruz. İlave olarak da çeşitli güvenlik firmalarının inhouse denilen yerel yazılımlarından da istifade ederek güvenlik seviyemizi üst seviyede tutmaya çalışıyoruz. Aynı yöntemi yakın zamanda tüm İspark otoparklarının İstanbul Kart ile çalışmaya başlamasıyla arttırarak devam edeceğiz. Zira İstanbul Kart entegrasyonu ile İspark otoparkına araçlarını park edenler yoluna toplu taşıma araçları ile ve indirimli olarak devam edebilecekler. Bu hizmeti sağlarken İstanbul Kart operasyonunu yürüten yine İBB şirketi Belbim A.Ş. ile ortak entegrasyon ve güvenlik çalışmaları yaparak kullanıma başlanmasından sonraki güvenlik açıkları ihtimallerini tespit ediyoruz. Daha sonra da bu ihtimaller üzerinden gerekli tedbirleri alarak hizmete başlamış olacağız ve sonrasında sahadaki uygulamaya göre güvenlik tedbirlerimizi sık sık tekrarlayacağız. İstanbul Kart en fazla 20 Milyon insan tarafından kullanır düşüncesiyle yukarıda bahsettiğim araçları kullanmaya devam edeceğiz ve bu minvalde eksiklerimiz varsa da onları görmüş olacağız. Bu konuya önem veriyoruz çünkü bir İstanbullunun dediği gibi, “Benim 7 Özel Aracım var ama 1 Tane Anahtarım Var o da İstanbul Kart”.

KAYNAKLAR

Ashe, J. P., (2004), “A Vulnerability Assessment of the East Tennessee State University Administrative Computer Network”, East Tennessee State University, Electronic Theses and Dissertations. Paper 858. http://dc.etsu.edu/etd/858

Önal, H., (2010), Güvenlik Testlerinde Açık Kodlu Araçların Kullanımı. Bilgi Güvenliği Akademisi. 04.07.2016, http://www.bga.com.tr/

Soğukpınar, İ., (2010), Veri ve Ağ Güvenliği Ders Notları, Gebze Yüksek Teknoloji Enstitüsü.

https://www.netsparker.com/. [15.06.2017].