T.C. İSTANBUL TİCARET
ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL İŞLETMELERDE BİLGİ VE VERİ GÜVENLİĞİ

ÖMER FARUK KAYA
1460Y63105

YÜKSEK LİSANS TEZİ
SİBER GÜVENLİK ANABİLİM DALI
İSTANBUL, TEMMUZ 2017

T.C. İSTANBUL TİCARET

ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL İŞLETMELERDE BİLGİ VE VERİ GÜVENLİĞİ

DANIŞMAN

YRD DOÇ DR. ERDİNÇ ÖZTÜRK

ÖMER FARUK KAYA

1460Y63105

YÜKSEK LİSANS TEZİ
SİBER GÜVENLİK ANABİLİM DALI
İSTANBUL, TEMMUZ 2017

KABUL VE ONAY SAYFASI

Ömer Faruk KAYA tarafından hazırlanan **Kurumsal İşletmelerde Bilgi ve Veri Güvenliği** adlı tez çalışması 20../07../2017 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü **Siber Güvenlik Anabilim Dalı**'nda yüksek lisans tezi olarak kabul edilmiştir.

	Adı-Soyadı	İmza
Danışmanı	**: Yrd. Doç. Dr. Erdinç ÖZTÜRK**	
Jüri Üyesi	**: Yrd. Doç. Dr. Muhammed Ali AYDIN**	
Jüri Üyesi	**: Yrd. Doç. Dr. Ali BOYACI**	

Onay Tarihi : 15./08./2017

Yrd. Doç. Dr. Berk AYVAZ

Enstitü Md. V.

AKADEMİK VE ETİK KURALLARA
UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

15/08/2017

Ömer Faruk KAYA

İÇİNDEKİLER

ÖZET

Günümüzde artık bir yaşam biçimi halini alan bilgisayar dünyasında dosyaları, bilgileri özetle veriyi korumak en önemli konu olarak karşımıza çıkıyor. Özellikle paylaşımlı ve halka açık iletişim sistemlerinde veri güvenliği daha da fazla önem arz ediyor.

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 gerekenlerin vurgulanması hedeflenmiştir. Ayrıca, İstanbulkart'ın İspark uygulamalarına entegrasyonu sırasında bu önlemlerin uygulanması ile ortaya çıkan güçlükler ve sonuçlar bu çalışma ile sunulmuştur.

ABSTRACT

Nowadays, it is the most important issue to protect the computer files of the world, which is now a life style, and to keep the information summarized. It is especially important in shared and public communication systems.

Another important message is that it is vital to protect data in the communication methods provided by the users and the center-to-center communication protocols. Network security precautions are based on the protection of the transmission of the grant. In this study, especially in a public institution with a field location close to 150, the observation of the connection with the field and data security and emphasizing the need to be taken in the center. In addition, the difficulties and consequences of the implementation of these measures during the integration of Istanbul Card into Ispark applications are presented in this study.

TEŞEKKÜR

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda ve literatür araştırmalarımda yardımcı olan değerli Danışman Hocam Yrd. Doç. Dr. Erdinç ÖZTÜRK'e teşekkürlerimi sunarım. Yine Literatür araştırmalarımda yardımcı olan değerli arkadaşım Tamer ŞAHİN'e teşekkür ederim.

Tezimin yazım aşamasındaki desteklerinden dolayı İSPARK AŞ'ye teşekkür ederim.

Tezimin her aşamasında beni yalnız bırakmayan aileme sonsuz sevgi ve saygılarımı sunarım.

Ömer Faruk KAYA

İSTANBUL 2017

ŞEKİLLER

TABLOLAR

KISALTMALAR

AES : Advanced Encryption Standard, Gelişmiş Şifreleme Standardı
CAT TP : Card Application Toolkit Transport Protocol, Kart Uygulama Aracı İletişim Protokolü
ECC : Ecliptic Curve Cryptography, Eliptik Eğri Kriptografisi
EFS : Encrypted File System, Şifrelenmiş Dosya Sistemi
ETSI : European Telecommunications Standards Institue
HSM : Hardware Security Module, Güvenli Donanım Modülü
http : Hypertext Transfer Protocol, Hypertext Transfer Protokolü
MD5 : Message-Digest Algorithm 5, Mesaj-Özet Algoritması 5
MNO : Mobile Network Operator, Mobil Ağ Operator
NFC : Near Field Communication, Yakın Alan İletişimi
OTA : Over The Air, Hava üzerinden
POS : Point Of Sale, Satış Noktası
RFID : Radio Frequency Identification, Radyo Frekans
RSA : Rivest – Shamir - Adleman
SD : Security Domain, Güvenli Alan
SHA : Secure Hash Algorithm, Güvenli Karma Algoritması
SMS : Short Message Services, Kısa Mesaj Servisi
SP : Servis Provider, Servis Sağlayıcı
TSM : Trusted Service Manager, Güvenli Servis Yönetimi
UAC : User Account Control, Kullanıcı Hesap Denetimi
UICC : Universal Integrated Circuit Card, Entegre Devre kart
WEP : Wired Equivalent Privacy, Kabloya Eşdeğer Mahremiyet
WPA : Wi-Fi Protected Access, Wi-Fi Korumalı Erişim
BIOS : Basic İnput/Output System, Temel Giriş/Çıkış Sistemi
DNS : Domain Name System, Alan İsmi Sistemi
SSID : Service Set Identifier, Servis Seti Tanımlayıcısı

DHCP : Dynamic Host Configuraiton Protocol, Dinamik Bilgisayar Konfigürasyon Protokolü

NASL : Nessus Attack Scripting Language/ Nessus Saldırı Senaryosu Dili

JTR : John The Ripper, Parola Çözme Yazılım Aracı

GUI : Graphical User Interface, Grafiksel Kullanıcı Arayüzü

IPS : In-Plane Switching, Düzlem Geçişi

LFI : Local File Include, Yerelden Dosya Eklemek

RFI : Remote File Include, Uzaktan Dosya Eklemek

LAN : Local Area Network, Yerel Alan Ağı

MITM : Man in the Middle, Ortadaki Adam Saldırısı

EPC : Event Process Chain, Olay Süreç Zinciri

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 [1].

- **Gizlilik:** Verilerin başkaları tarafından görüntülenmesinin istenilmemesi
- **Bütünlük:** Verilerin başkaları tarafından değiştirilmesi istenilmemesi
- **Kullanım:** 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

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. Bu varsayım kurum içinde kullanılan cep telefonları ve mobil cihazlar içinde geçerlidir [2]. Bunun için de öncelikle varlıklarımıza karşı gelebilecek risklerin analizi yapılmalıdır.

2.1. Veri Güvenliği

Veri güvenliği, disk, iletişim ağı, yedekleme ünitesi ya da başka bir yerde tutulan verilerin, programların ve her türlü bilginin korunmasını ifade eder.

Bu koruma sadece tek bir yönde düşünülmemelidir. Veri güvenliğinin 3 ana boyutu vardır. Fiziksel güvenlik; çalınma, düşme gibi dış etkenlerden dolayı hasar görme risklerini kapsar [1]. Bilgisayar güvenliği ile, bilgisayara fiziksel olarak erişen yerel kullanıcıların yetki denetimlerinden, sistem arızalarına kadar uzanan geniş bir koruma perspektifini ifade eder.

İletişim güvenliği ise, ister yerel ağ düzeyinde, ister internet düzeyinde olsun bilgisayarlar arası iletişimden doğan tehditler ile ilgilenir.

2.1.1. Tehdit sınıflandırmaları

Bilgisayarlara yönelik tehditler, kaynaklarına ve türlerine göre sınıflandırılabilir. Tehditlerin kaynağı, teknik saldırılar, kötü niyetli kişi saldırıları, sistem hataları veya yangın, su baskını, terör gibi dış etkenler olabilir.

Tehdit türleri ise para hırsızlığı, yazılıma zarar verilmesi, bilgi çalınması, bilgiye zarar verilmesi, servislerin izinsiz kullanılması, zarar vermeden güvenlik ihlali ve sistemlerin kısmen veya tamamen devre dışı kalması olarak sayılabilir.

Bazı tehditlerin bu açıdan önemsiz olarak değerlendirilmesi ise büyük bir hata olacaktır [3]. Zarar vermeden güvenlik ihlali yapılan bir sistem, aynı zamanda her türlü hasara da açık demektir.

Ayrıca sistemlerin kısmen veya tamamen devre dışı kalması, çok ciddi zaman maliyetlerine de sebep olabilir.

2.1.2. Saldırı yöntemleri

Günümüzde bilgisayara yönelik saldırıların çok sayıda türü vardır. En yaygın saldırı türü, virüsler, solucanlar ve truva atları gibi kötü amaçlı yazılımlardır. Bir sonraki önemli tehdit yazılım açıkları ve arka kapılardır [4].

DoS saldırıları ile sistemi aşırı yükle bloke etme,

Somut hasar hedefleri olan mantıksal bombalar,

Phishing saldırıları, oltalama saldırıları

IP spoofing saldırıları, IP gizleyerek yapılan saldırılar

Host dosyasının çalınması,

Sosyal mühendislik ile aldatılma,

Mesajlaşma yazılımları ve internet trafiğinin izlenmesi,

Ve şifre kırma sistemleri, diğer saldırı yöntemleri olarak sayılabilir.

2.1.3. Korunma yöntemleri

Bilgisayara yönelik saldırılar ve tehditler karşısında, elbette çok sayıda da korunma yöntemi söz konusudur.

Kimlik doğrulaması, güvenlik yazılımları, yazılım güncellemeleri, verilerin yedeklenmesi, veri erişim izinleri, verilerin şifrelenmesi ve güvenli silme bu kapsamda ele alınacak başlıklardır. Ancak kullanıcının eğitimi, saldırılara karşı korunmada en iyi yöntemdir.

2.1.3.1. Kimlik doğrulaması ve şifreler

Kimlik doğrulamasında en yaygın yöntem şifrelerdir. Şifreler belirli bir kullanıcı adına bağlı olarak girilebileceği gibi, kullanıcı adı olmaksızın sadece şifre ile koruma sağlayan sistemler de bulunmaktadır..
Kimlik doğrulamasının işe yaraması, yani güvenlik sağlaması için, güçlü bir şifrenin oluşturulması ve bu şifrenin iyi korunması zorunludur.
Dünyada aşılması "imkansız" bir şifre yoktur. Ancak aşılması imkansıza yakın derecede zor olan şifreler vardır [4]. Şekil 2.1.3.1de örnek şifreler gösterilmiştir.

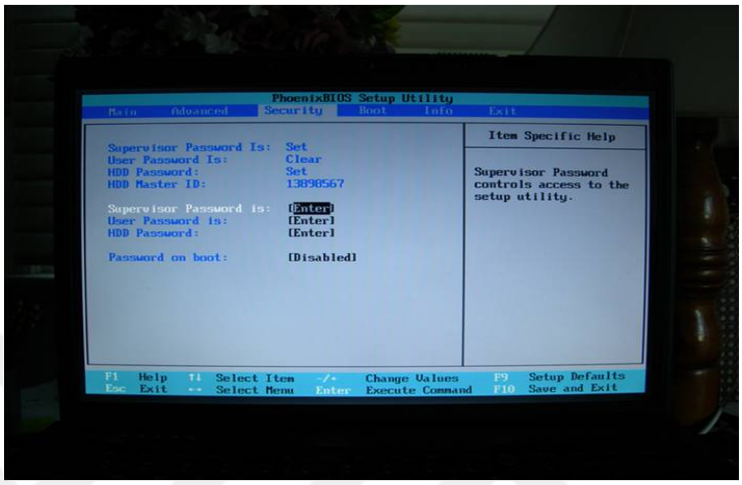
Örnek Şifreler	Değerlendirme
123456	İnanılmaz kolay; aynı zamanda en yaygın kullanılan şifre
Jocrian7	Güçlü ve kırılması zaman alan bir şifre
This1sV#ryS3cure	Çok güçlü ve kırılması çok zor olan bir şifre

Şekil 2.1.3.2. Şifre örnekleri

2.1.3.2. BIOS şifreleri

Bilgisayara koyabileceğiniz ilk şifreler BIOS şifreleridir. Çoğu BIOS yazılımında, BIOS ayarlarını değiştirebilmek ve bilgisayarı açmak için 2 ayrı şifre belirlenebilmektedir.

Bu şifreler fiziksel erişim imkanı bulunan kişiler için anlamlıdır. Yani bu şifreler herhangi bir ağ veya internet güvenliği sunmaz. Ayrıca yetkisiz kişi sistem kasasını açabilecek durumda olursa, BIOS şifrelerini geçersiz kılması son derece kolaydır. Buradaki koruma, çok güçlü bir güvenlik sağlamasa da, basit şekilde erişimlerin önünün kesmekte idealdir. Şekil 2.1.3.3.1 de BIOS şifre bölümü gösterilmiştir.



Şekil 2.1.3.4.1. BIOS şifre bölümü

2.1.3.3. Drivelock denetimi şifresi

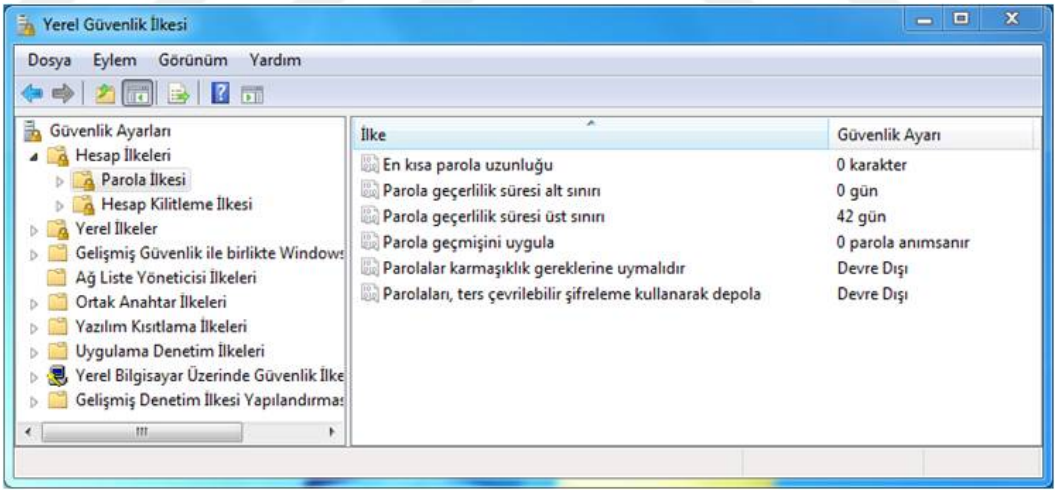
DriveLock denetimi ise, özellikle taşınabilir bilgisayarlarda kullanılan bir sistemdir. Etkinleştirilmesi durumunda, bilgisayarın önyüklemesi sırasında kullanıcının hard disk için şifre girmesi istenir. Yanlış şifre girilirse sürücü kilitlenir ve önyükleme yapılamaz. Bu koruma, özellikle bilgisayarın çalınması durumunda kritik verilerinizin güvenliği açısından önemlidir. Eğer bilgisayarın bu özelliği varsa, bu da BIOS üzerinden yapılandırılır. Şekil 2.1.3.5.1de DriveLock şifreleme yöntemi gösterilmiştir.

Şekil 2.1.3.6.1. DriveLock şifreleme örneği

2.1.3.4. Windows Kullanıcı Hesabı Şifreleri

Windows erişimi için bir kullanıcı hesabı adı ve şifresi gereklidir. Kullanıcı hesabı şifresi sadece oturum denetimi sunar; verileri şifrelemez. Eğer kullanıcı isterse, kullanıcı hesabını şifresiz olarak da kullanabilir; ancak bu ciddi bir güvenlik açığı kabul edilir. Aynı zamanda bazı ağ servisleri de, şifresiz hesaplarla çalışmayacaktır. Denetim masası, yönetimsel araçlar dizininde bulunan yerel güvenlik ilkelerinden, kullanıcı hesabı parolalarının tabi olacağı kurallar değiştirilebilir. Şekil 2.1.3.4.1.'de olduğu gibi buradan en kısa parola limiti koyabilir, parolanın maksimum ve minimum geçerlilik süresini belirleyebilirsiniz. Tekrar kullanım limiti ise, geçişte kullandığınız parolayı tekrar kullanmanız için arada değiştirmeniz gereken parola sayısını ifade eder. Karmaşıklık derecesini zorunlu tutarsanız, parolalarda harf ve rakamın bir arada kullanılması gibi zorunluluklar aranır.

Windows normalde parolaları geri dönüştürülemez şekilde kaydeder. Ancak kullanıcı isterse, özel durumlar için parolaların ters çevrilebilir şifrelemeler ile depolamasına da izin verebilir.



Şekil 2.1.3.7.1. Windows şifreleme yönetim ekranı

2.1.3.4. Windows şifrelerinin sınırları

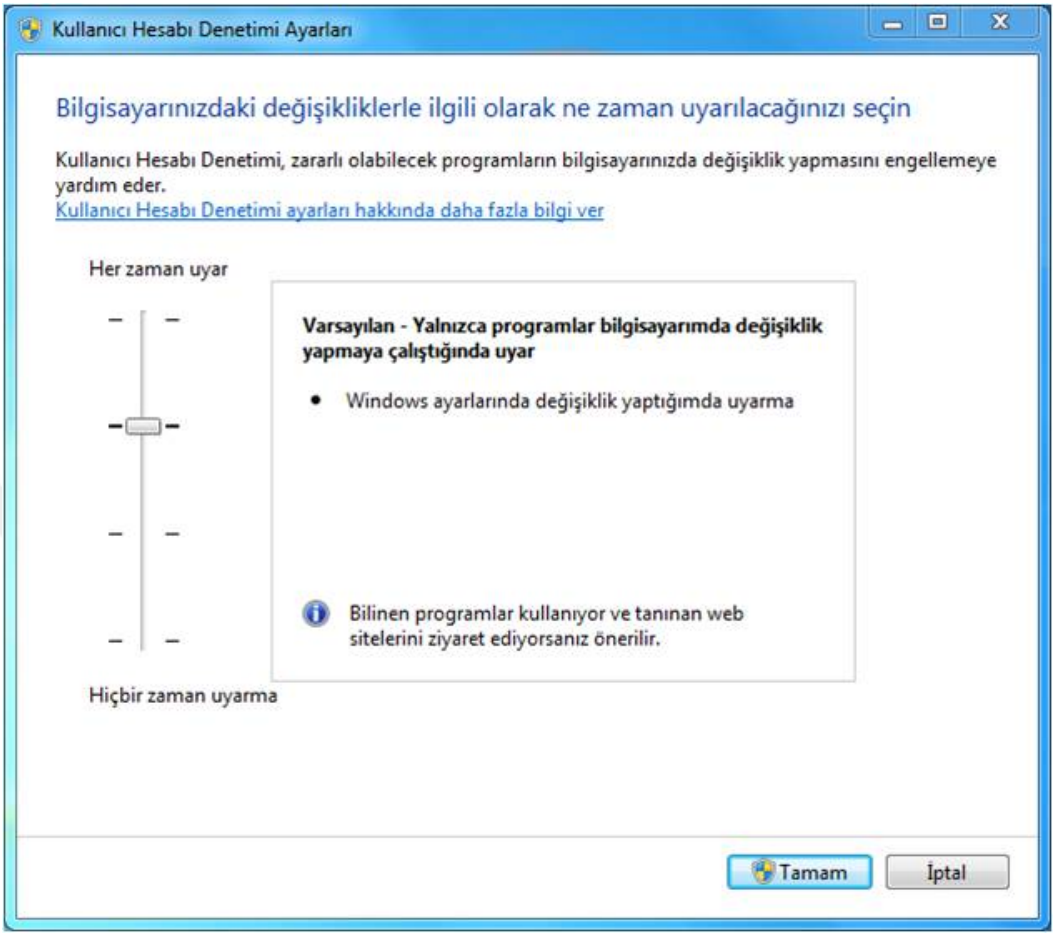
Windows kullanıcı hesaplarının şifrelenmesi sadece oturum denetimi sunduğunu, sabit disk üzerinde bulunan verileri ise şifrelemediğini söylemiştik. Bu sebeple, Windows hesabına şifre koysanız dahi, sabit diskiniz başka bir PC'ye takıldığında bu şifre bir anlam ifade etmeyecektir. Ayrıca bilgisayarı CD sürücüsünden başlatma imkanı olan bir kişi, özel bir yazılım ile Windows kullanıcı hesabı şifresinin üzerine yazabilir, şifreyi silebilir veya yedekleyebilir. Yapamayacağı tek şey, şifrenin ne olduğunu öğrenmektir. Bize fark ettirmeden güvenliğinizi aşmaya çalışan bir kişi, öncelikle oturum şifrenizi bir flash bellek veya diskete yedekleyebilir. Daha sonra şifreyi silip oturumunuzu açarak; işini bitirdikten sonra da yedeklenilen şifreyi geri yükler. Bu sayede siz birisinin sisteminize girdiğini hiçbir şekilde anlamayabilirsiniz. Bu yazılım aracının tek iyi tarafı, şifresi kaybolmuş sistemlerde kurtarma amaçlı olarak kullanabilmesidir. Kullanıcılar, Windows şifrelerinin sınırlarını iyi bilmelidir; kendisini sonsuz güvende hissetmek bir kullanıcının en zayıf noktası olacaktır.

2.1.3.5. UAC: Kullanıcı Hesabı Denetimi

Kullanıcı hesabı denetimi, sadece Windows Vista, Windows 7 ve sonraki sürümlerinde bulunan bir özelliktir.

Yönetimsel yetki gerektiren bir işlem söz konusu olduğunda, bu işlem güvenli bir masaüstü ile kullanıcıya iletilir ve kullanıcının onayı istenir. Bu her ne kadar güzel bir koruma sistemi gibi görünse de, Windows Vista'da kullanıcıyı bunaltacak düzeyde uyarılar vermesiyle çoğu kullanıcı tarafından pasif duruma getirilmiştir. Windows 7'de ise birçok açıdan düzenlenmiş ve sadece gerçekten önemli işlemlerde uyarı vermesi sağlanmıştır. Windows 10'da ise yerel hesap denetimleri kullanıcının işini daha kolay hale getirmiştir.

Windows 7'de kullanıcı hesapları kısmından uyarı düzeyleri yönetilebilirken, Windows Vista'da sadece bu denetim açık veya kapalı duruma getirilebiliyordu.



Şekil 2.1.3.8.1. Kullanıcı hesabı denetim ekranı

2.1.3.5 Akıllı kartlar

Şekil 2.1.3.5.1.'da yer alan akıllı kartlar, kimlik doğrulamasında kullanılan ikinci yöntemdir. "Kişinin sahip olduğu bir şey" kategorisine giren bu kartlar bir kredi kartı yapısındadır ve veri depolanabilen bir çipe sahiptir. Bu çip üzerinde kullanıcı kimliğini tanımlayan veriler bulunur. Gelişmiş akıllı kartlar ileri düzey şifreleme algoritmaları kullanan özelleştirilmiş donanıma sahiptirler.

Bugün Maliye Bakanlığı gibi bazı kamu kuruluşları, Tübitak tarafından geliştirilen akıllı kartlar ile dijital imza kullanımını kabul etmektedirler.

Şekil 2.1.3.5.1. Akıllı kartlar

2.1.3.6. Biometrik aygıtlar

Şekil 2.1.3.6.1.'da örnekleri verilen biometrik aygıtlar, parmak izleri, retina ve iris örüntüleri ile kemik yapısı gibi bedensel özellikleri algılayan aygıtlardır. Günümüzde parmak izi tarayıcıları taşınabilir bilgisayarlar veya USB aygıtlarında yaygın biçimde kullanılmaya başlamıştır.

Windows oturum açma şifresi yerine parmak izinizi kullanmanız bile mümkündür. Havaalanı veya devlet kurumları gibi ortamlarda ise, daha gelişmiş biometrik okuyucu sistemleri kullanılmaktadır.

Şekil 2.1.3.6.1. Biometrik aygıtlar

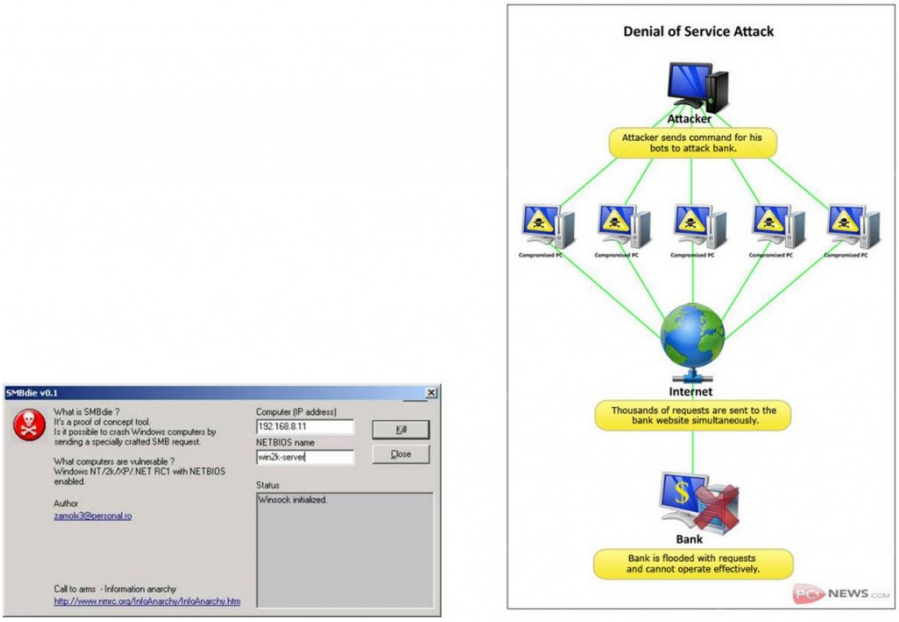
2.1.4. Yazılım açıkları ve arka kapılar

Yazılım açıkları ve arka kapıların oluşturduğu tehditler, herhangi bir istenmeyen zararlı yazılımın sisteminize bulaşmasına bağlı değildir. Yazılımda bulunan bir kod düzeni, yetkisi olmadığı halde bir kullanıcının üstün yetkilerle sisteme müdahale etmesini sağlayabilmektedir [5].

Eğer bu bilinçli yerleştirilmiş bir işlem noktası ise, arka kapı; eğer yanlışlıkla unutulmuş bir işlev ise yazılım açığı olarak tanımlanır. Örneğin yoğun kullanıldığı dönemlerde mIRC scriptleri bolca güvenlik açığı bulunan yazılımlardı. Hatta bazıları, bilinçli yerleştirilmiş arka kapılardı.

2.1.5. DoS: denial of service

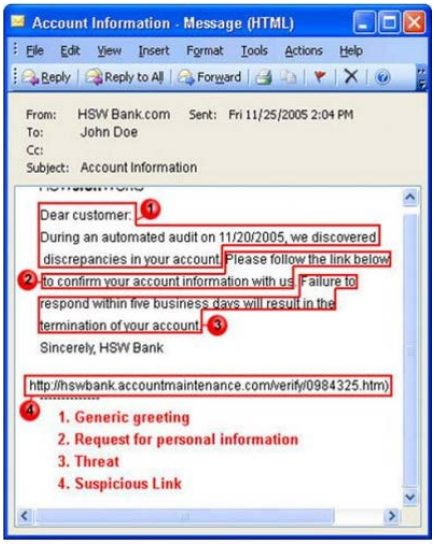
Şekil 2.1.5.1.'de yer alan Denial of Service kelimelerinin kısaltmasından oluşan DoS ifadesi ile bilinen saldırılarda sistem veya programlara virüs bulaşmaz. Saldırının amacı, hedef sistemi aşırı yükleme ile bloke etmeye dayanır. Örneğin 10 dakika içinde 100.000 e-posta gelmesi durumunda e-posta hizmeti veren sunucular işlevlerini göremez hale gelebilir. Saldırı türünden de anlaşılacağı üzere bu saldırı verilere ciddi bir zarar vermez; ancak bir web sitesinin yayının kesilmesi, çok daha önemli bir kayıp olabilir.



Şekil 2.1.5.1. Denial of Service

2.1.6. Phishing - oltalama

Phishing yani oltalama yöntemi, kullanıcının benzerlik ile kandırılmasına dayanır. Bir internet sitesinin veya e-posta mesajlarındaki gönderen adının, benzer bir isim kullanılarak taklit edilmesidir. Kişilerin gizli şifre ve mali bilgilerini elde etmeyi hedefler. Özellikle bankalardan geliyormuş gibi görünen e-posta mesajları ve banka web tasarımlarının kopyalandığı sahte banka web siteleri son zamanlarda çok yaygın görülmektedir.



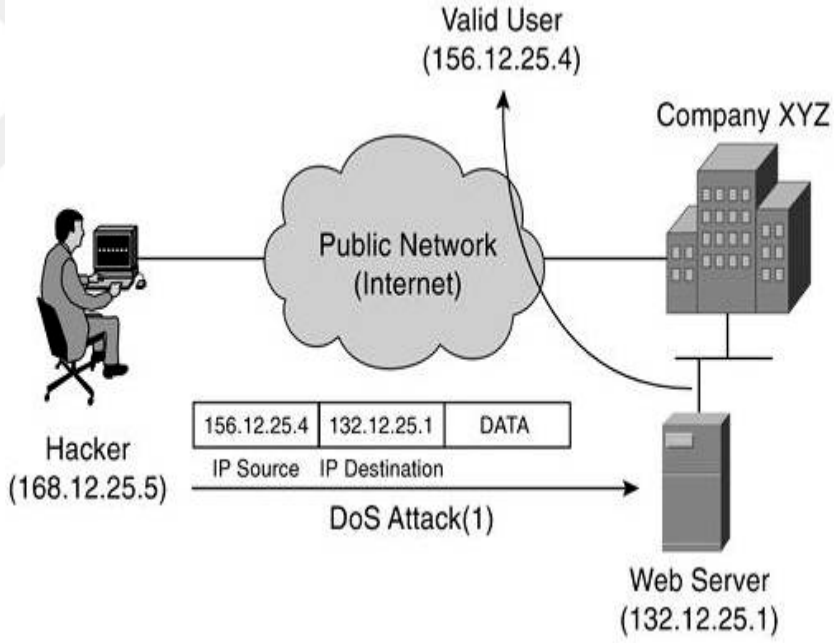
Şekil 2.1.6.1. Phishing ekranı

2.1.7. IP spoofing – ıp gizleme,yanıltma,sızdırma

Bir hedef IP adresine başka bir IP adresinden geliniyormuş gibi bağlantı sağlanması işlemine IP Spoofing denilir. Günlük kullanımda IP adresinin çalınması olarak da bilinir.

Proxy sunucular üzerinden bağlanmak gibi çeşitleri olsa da gerçek IP spoofing giden paketlerdeki kaynak adresi değiştirerek yapılır. Spoofing terimi, yanıltma anlamı ile diğer birçok internet tabanlı tehdit için de kullanılır; ancak daha çok IP Spoofing terimi ile kullanımı yaygındır.

Örneğin DNS spoofing veya e-mail spoofing tabirlerini de duymak oldukça mümkün.

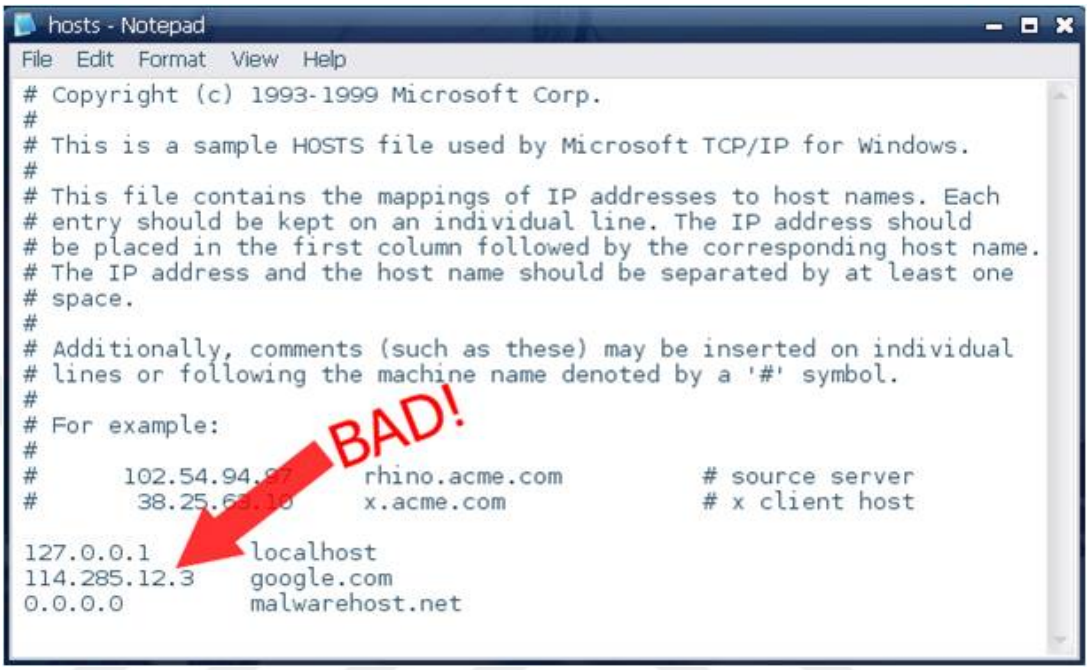


Şekil 2.1.7.1. IP spoofing ağı

2.1.8. Host dosyasının çalınması

Bilgisayarınız web sunucu isimlerini host dosyasından ve devamında DNS sunucuları üzerinden öğrenir. Eğer host dosyanızın içeriği değiştirilmiş veya bilgisayarınızı güvenli olmayan bir DNS veya Proxy sunucusuna yönlendirilmiş ise, gerçek olmayan web sitelerine gitme ihtimaliniz vardır.

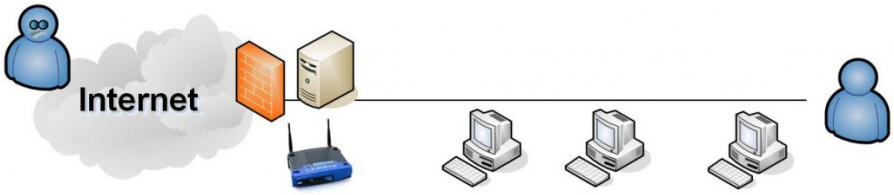
Yani eğer bir şekilde yanlış bir isim çözümlemesi yapılırsa, gerçek bankanın değil, taklit bankanın web sitesine gidilebilir. Phishing saldırısından dikkatli davranarak kurtululabilir; ancak host dosyasında, bunu anlamak çok daha zordur. Güvenlik yazılımları host dosyasını bu durumlar için takip ederler. DNS sunucular için ise, internette her bulduğunuz her sunucu IP adresine güvenilmemelidir.



Şekil 2.1.8.1. Host dosyası

2.1.9. Firewall: güvenlik duvarları

Güvenlik duvarları, bilgisayarın veya ağların, ağ ve internet ortamı ile iletişimini takip eden ve tanımlı kurallara göre bu trafiği yöneten yazılımlardır. Kurumsal alanlarda genellikle ağın internet çıkışında bulunurken, bilgisayarlar da özel yazılım olarak da bulunabilir. Bir güvenli duvarı yazılımı, izin verilenler dışındaki tüm portlar kapatır. Açık olan portlar üzerindeki paket trafiği ise sıkı kurallar tarafından denetlenir. Windows tüm işletim sistemlerinde yerleşik güvenlik duvarı bulundurmaktadır.



Şekil 2.1.9.1. Windows güvenlik duvarı yapısı

2.1.10. Verilerin şifrelenmesi

Şifreleme, verilerin bir algoritma ile, doğru anahtara sahip olunmadığı sürece okunamaz hale getirilmiş olmasıdır. Bu anahtar okuma veya değiştirme şifresi gibi tanımlarla da ifade edilir. Eğer şifreleme ve şifrelenmiş veriyi okuma işlemleri aynı anahtar ile gerçekleşiyor ise simetrik şifreleme yapılmıştır. Birazdan bazılarına değineceğimiz EFS, BitLocker, WEP, WPA, Kerberos, AES gibi şifreleme sistemleri simetrik şifreleme yaparlar. Eğer verinin şifrelenmesi için ortak, verinin okunması için ise özel olarak 2 anahtar var ise, asimetrik şifreleme yapılmıştır. RSA ve ECC en yaygın kullanılan asimetrik şifreleme teknikleridir.

Asimetrik anahtar kullanımı kesinlikle daha güvenli, ancak çok daha karmaşıktır. Asimetrik şifreleme için hafızada tutulamayacak, hatta elle yazılamayacak yapıda anahtarlar kullanılır. Asimetrik şifreleme genelde kurumsal veri aktarım sistemlerinde, iletişim kanallarının güvenliğinde kullanılır.

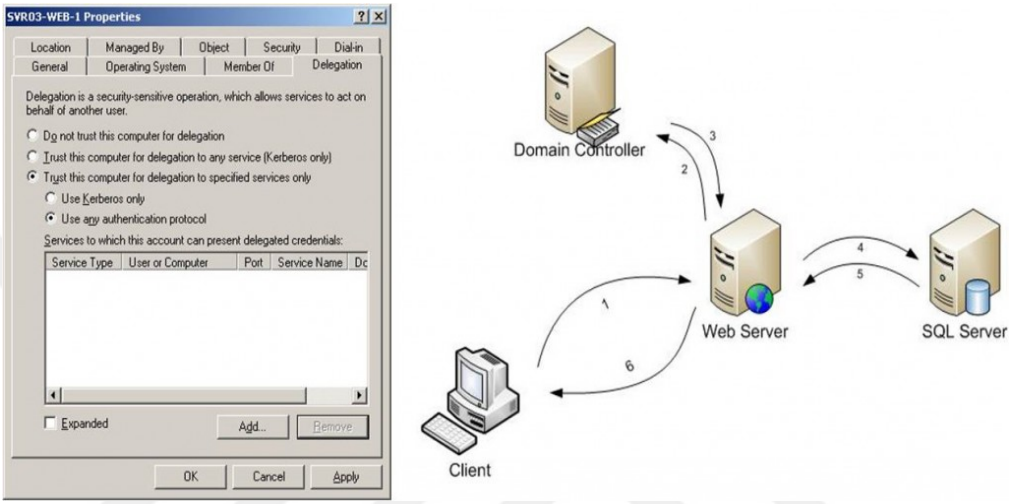
2.1.11. Bütünlük doğrulama şifrelemeleri

Bütünlük doğrulama şifrelemeleri ise, matematiksel olarak oluşturulmuş sayılardır ve geri dönüşü olacak şekilde çözülemezler. Daha çok indirilen dosyaların bütünlüğünün kontrolü veya veri tabanlarında şifrelerin saklanması işlevlerinde kullanılırlar.

SHA ve MD5 en bilinen bütünlük doğrulama şifreleme yöntemleridir. Siz bir sitede oturum açmak istediğiniz şifreniz MD5'e dönüştürülür ve daha önce oluşturulan MD5 ile karşılaştırılır. Bu sayede site yöneticileri bile girdiğiniz şifreleri öğrenemezler.

2.1.12. Ağ kimlik doğrulaması

Veri şifreleme yöntemlerine bir örnek kullanım da Windows'un ağ kimlik doğrulama işlevidir. Windows'ta network için oturum açtığınız zaman kimlik doğrulaması Kerberos protokolü ile korunmaktadır. Bu koruma, ağ boyunca kimlik doğrulaması yapılacak şekilde kullanıcı adı ve şifresi için koruma katmanı sağlamış olur.



Şekil 2.1.9 Veri kimlik doğrulama şeması

2.1.13. Potansiyel güvenlik açığı bulunduran yazılımlar

Bazı yazılımlar, güvenlik tehditleri içeren yapılandırmalar gerçekleştirirler ve kullanıcılar bunun farkında olamayabilirler.

Veya daha önce bahsettiğimiz gibi bizzat kendilerinde güvenlik açıkları veya arka kapılar varolabilir.

Şekil 2.1.13.1.'de gösterilen P2P yazılımları, whatsapp vb. sohbet platformları, bir zararlı yazılım olmamakla beraber çalışma mantıkları gereği güvenlik zafiyetleri bulunan yazılımlardır.

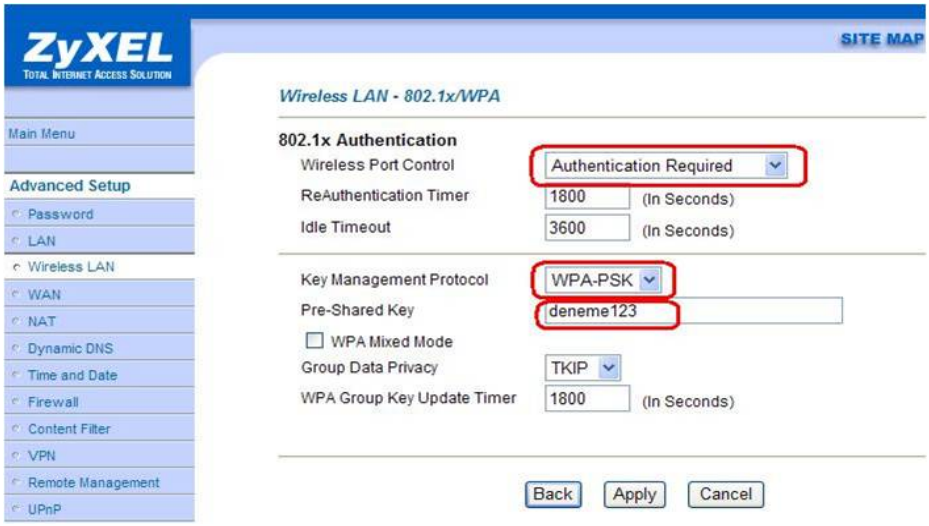
Bu yazılımlar çalışmaları için gerekli olan sistemler sebebiyle kullanıldıkları bilgisayarı saldırıya açık hale getirebilmektedirler.

Zorunlu olmadıkça kullanıcılar bu yazılımlardan uzak tutulmalı; hatta iş yerinde bu tip yazılımların kullanımına kesinlikle müsaade edilmemelidir..

Şekil 2.1.13.1. P2P yazılımları

2.1.14. Kablosuz bağlantılarda güvenlik tehditleri

Kişisel kullanıcı güvenliğinde günümüzde en çok güvenlik problemi yaşanan diğer bir konu da, kablosuz bağlantı güvenliğidir. Kablosuz modem ve diğer erişim noktaları mutlaka şifreli olmalı ve mümkün olduğu kadar WPA2 şifreleme yöntemi kullanılmalıdır. WPA2 kırılması çok daha zor olan bir şifreleme sistemidir. Ayrıca erişim noktasının SSID yayınlaması ve istemcilere DHCP servisi sunması da zorunlu olmadığı sürece kapatılmalıdır. Fabrika ayarında gelen erişim şifresi mutlaka değiştirilmelidir. Kullanıcıların %90'ı bunun farkında değildir. Bu sebeple IP adresi bilinen bir internet kullanıcısının modemine yetkili olarak erişmek, artık günümüzde basit hale gelmiştir. Yapılabilecek son güvenlik önlemi de MAC adresleri için filtre uygulanmasıdır. Bu sayede sadece sizin izin verdiğiniz MAC adresleri kablosuz ağınıza bağlanabilir.



Şekil 2.1.14.1. ZyXEL modem arayüz ekranı

2.1.15. Kurumsal veri sınıflandırması

Kurumsal alanda çeşitli veri sınıflandırmaları vardır. Kurumsal açıdan önemli verilere yetkisiz kişiler tarafından ulaşıldığında, güvenlik kaybına veya bir şirket için yararlı olmama ile sonuçlanabilir. ISO standardına göre veriler 5 ana sınıfa ayrılırlar; genel, dahili, ticari, gizli ve çok gizli. Bir diğer sınıflandırma yaklaşımına göre ise kategoriler genel, kişiye özel, hizmete özel, kuruma özel, gizli ve çok gizli olarak sayılır [18]. Askeri ve kamu hizmetleri alanında genellikle bu sınıflandırma yaklaşımı görülmektedir..

2.1.16. Önemli kurumsal güvenlik açıkları

Kurumsal alanda, bireysel bilgisayar kullanımından daha fazla ve daha ciddi güvenlik açıkları söz konusu olabilir [6].

- Hatalı kablosuz ağ yapılandırması
- Hatalı yapılandırılmış VPN sunucuları
- Web uygulamalarında yazılım açıkları ile SQL sorgularının değiştirilebilmesi
- Web uygulamalarında başka siteden kod çalıştırma
- Kolay tahmin edilebilir veya kırılabilir şifreler oluşturmak
- Güncellemeleri yapılmamış sunucular ve işletim sistemleri
- İşletim sistemi ve hazır uygulamaların standart ayarlarla kurulması
- Güvenlik duvarı tarafından korunmayan sistemler

Hatalı yapılandırılmış saldırı tespit sistemleri, önemli kurumsal güvenlik açıkları olarak sayılabilir [6].

2.1.17. Kurumsal güvenlik ihmalleri

Kurumsal alanda teknik güvenlik açıklarının yanı sıra, tehdit doğurabilecek önemli görev ihmalleri de olabilir.

En büyük ihmal, sorun çıkana kadar çözümün ertelenmesidir. Kurumsal bilginin ve prestijin maliyetinin kavranılamaması da ciddi bir problemdir. Bir çevrimiçi satış sitesinin yazılımsal açıklar sebebiyle hacker saldırısına kalması, o sitenin ticari hayatını bitirebilecek bir güven sarsılmasına sebep olabilir.

Bilgisayar güvenliğini yetersiz kişilere bırakmak ve sorumlu personelin eğitim süreçlerinin ihmal edilmesi de önemli bir etkendir. Sorumlu personelin kendilerini geliştirmesine imkân verecek şekilde iş yüklerinin dengelenmesi son derece önemlidir [6].

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 metot 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 testlerinin çeşitleri ve özellikleri açıklanmıştır. Devamında, hem açıklanan test araçlarından kullanılan hem de kendi oluşturduğumuz kütüphaneden faydalanarak ortaya çıkan uygulama ile ilgili bilgilere yer verilmiştir. Sonuç bölümde ise uygulama değerlendirmeleri ve sonuçlar tartışılmıştır.

4.1 Penetrasyon Testi

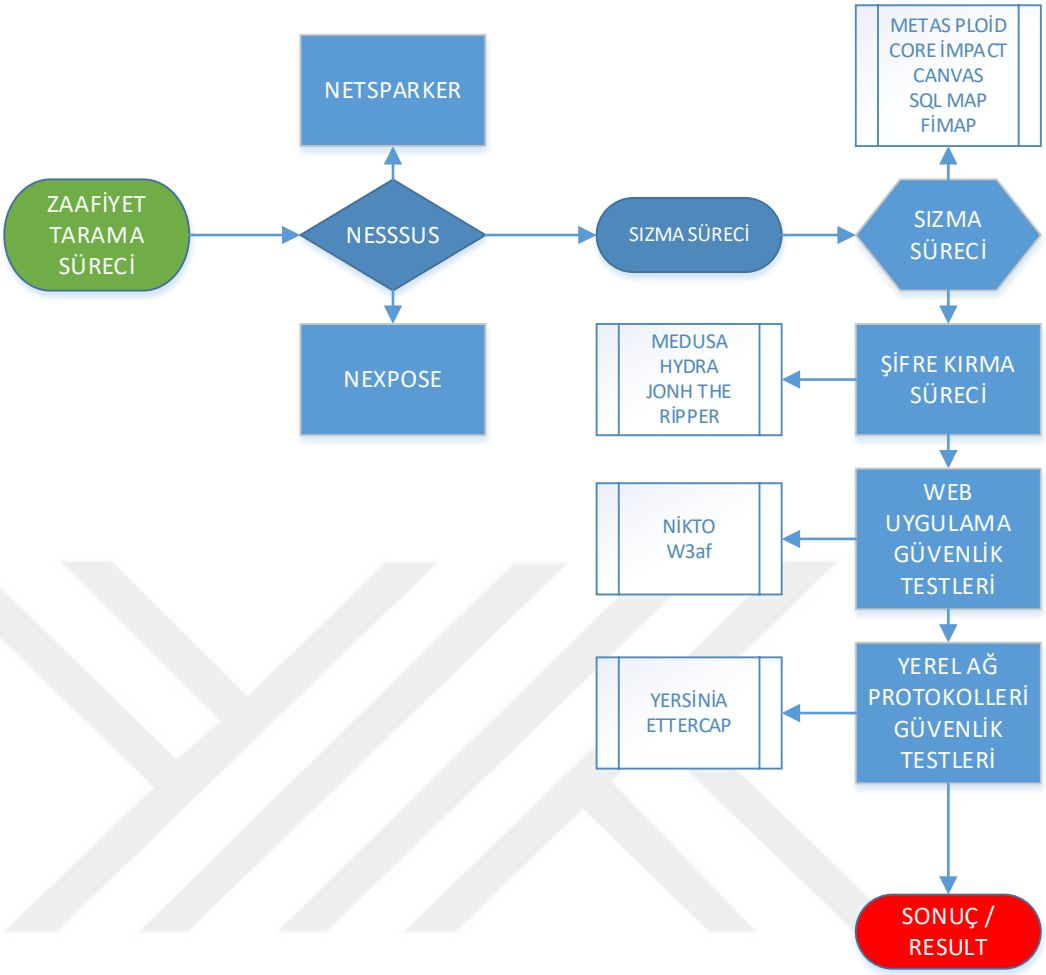
Temel olarak belirli güvenlik düzeyindeki ihlallerin bulunması ve ardından bu ihlallerin azaltılması, gereken adımların atılmasını sağlamak için var olan güvenlik mekanizmalarını denetleme ve bu mekanizmaları atlatma denemelerinden oluşur [7].

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 [7].

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 birçok 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 [8].

Penetrasyon testinin EPC (Event Process Chain) diyagramına göre olay süreç zinciri Şekil 4.2.1 de gösterildiği gibidir.



Şekil 4.2.1. Penetrasyon Süreç Zinciri

Penetrasyon testi;

- 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.

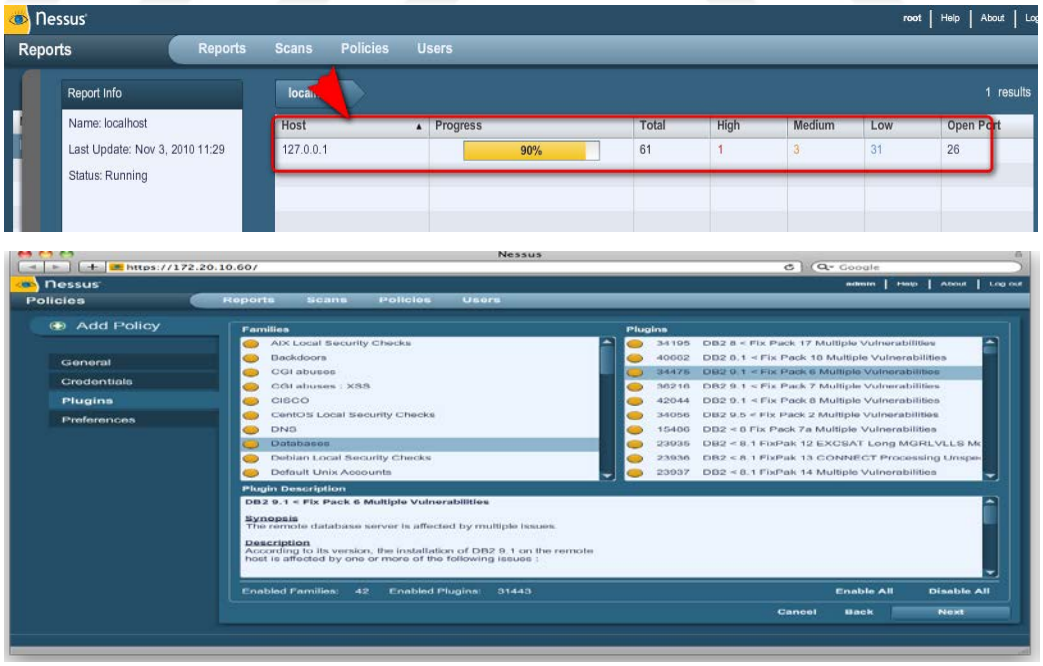
Zafiyet tarama süreçi ve kullanılan temel araçlar

Bu sürecin amacı belirlenen hedef sistemlerdeki açıklıkların ortaya çıkarılmasıdır. Bunun için sunucu servislerdeki bannerlar (afiş) ilk aşamada kullanılabilir. Ek olarak birden fazla zayıflık tarama aracı ile bu sistemler ayrı ayrı taranarak oluşabilecek false positive (yanlış pozitif) 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 araçları ön tanımlı ayarlarıyla farklı portlarda çalışan servisleri tam olarak belirleyememektedir.

4.2.1.1 Nessus

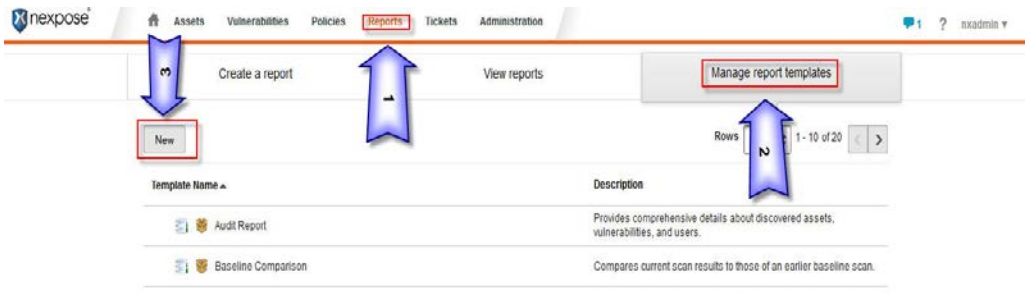
Şekil 4.2.1.1.1.'de gösterilen Nessus güvenlik camiasının ilk açık kod zafiyet tarayıcılarındandır. 3.x sürümüyle birlikte lisans modeli değişmiştir. Ücretsiz olarak ticari amaç harici kullanılabilir[9]. Piyasadaki en iyi açıklık tarayıcılardandır. Kendi açıklık tanımlama dili (NASL) sahiptir.



Şekil 4.2.1.1.1.Nessus

4.2.1.2 Nexpose

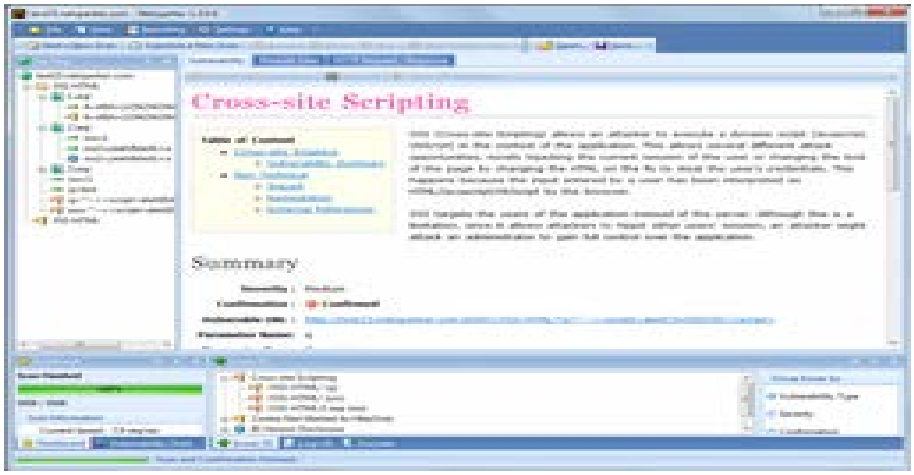
Rapid7 için çalışan Şekil.4.2.1.2.1.'de gösterilen Nexpose tüm güvenlik açığı yönetimi yaşam döngüsünü desteklemeyi amaçlayan bir güvenlik tarayıcısıdır [10]. Keşif, tespit, doğrulama, risk sınıflandırması, etki analizi, raporlama ve hafifletme bölümlerini içerir.



Şekil.4.2.1.2.1. Nexpose [10]

4.2.1.3 Netsparker

Şekil.4.2.1.3.1.'de yer alan Netsparker tespit ve güvenlik açılarından yararlanmayı da içeren bir web uygulama güvenliği tarayıcısıdır. Başarılı bir istismar sonrası teyit edilen açıklıkları raporlar aksi halde bulduğunu test eden bir araçtır.



Şekil.4.2.1.3.1. Netsparker

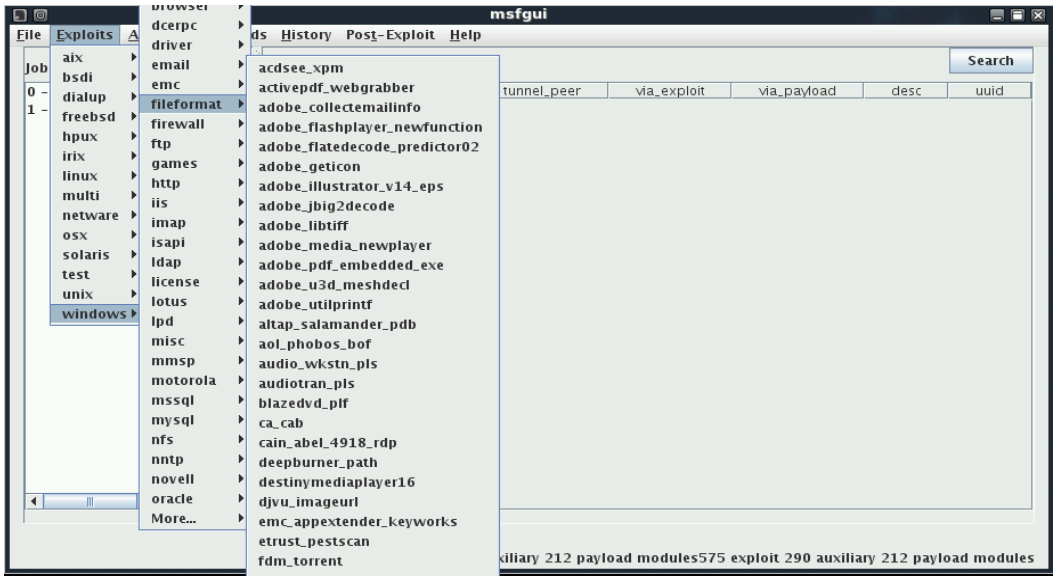
4.2.2 Sızma süreci ve kullanılan temel araçlar

Belirlenen açıklıklar için POC kodları/araçları belirlenerek denemeler başlatılabilinir. Açıklık için uygun araç yoksa ve imkan varsa ve test için yeteri kadar zaman verilmişse sıfırdan yazılması çok daha iyi olacaktır [10].

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. Zira aksi halde canlı sistem içerisinde yapılacak ilk işlem, sisteme geri dönüşü olmayan zararlar verebilecektir.

4.2.2.1 Metasploit

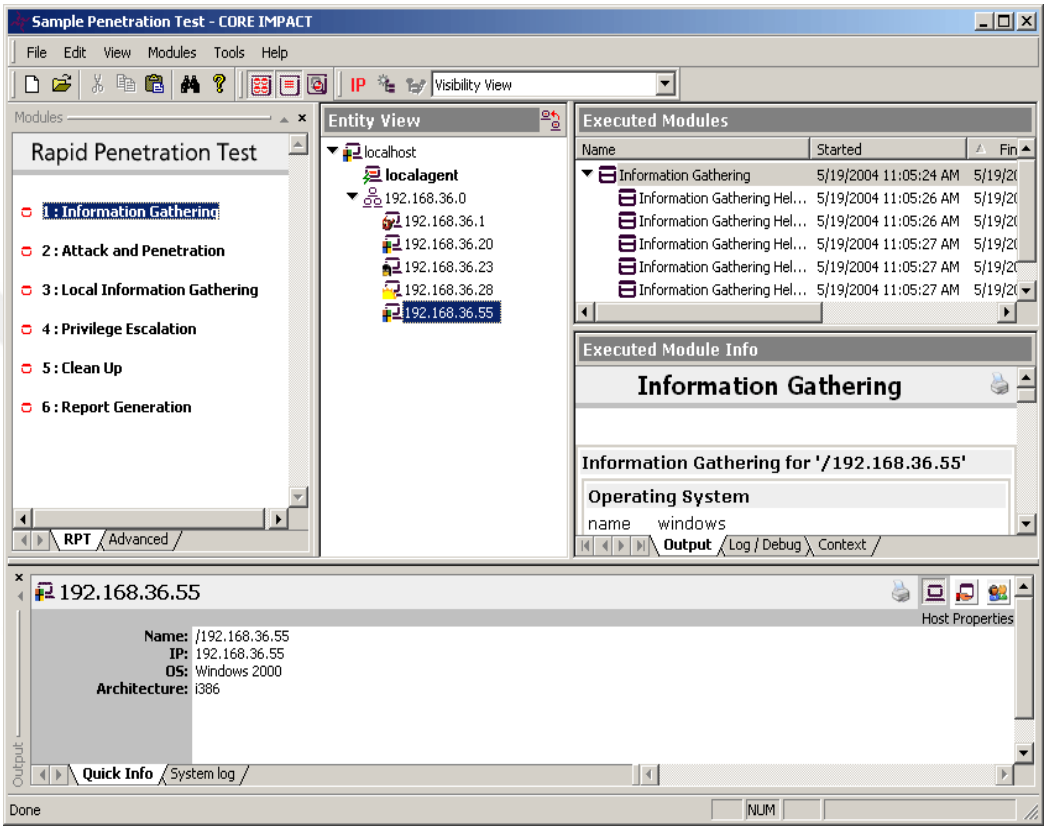
Şekil.4.2.2.1.1.'de gösterilen Metasploit, açık kaynak kodlu exploit geliştirme ve çalıştırma aracıdır. 600 civarı çalışan exploit barındırır. Aux modülleriyle bilgi toplama, ağ keşfi gibi işlemler gerçekleştirilebilir. Web, GUI ve konsoldan çalıştırılabilir. Gelişmiş AV, IPS atlatma özelliklerine sahiptir. Bir güvenlikçinin mutlaka kullanması gereken araçların başında gelir. Rapid7 firması tarafından satın alınmıştır.



Şekil.4.2.2.1.1. Metasploit

4.2.2.2 Core impact

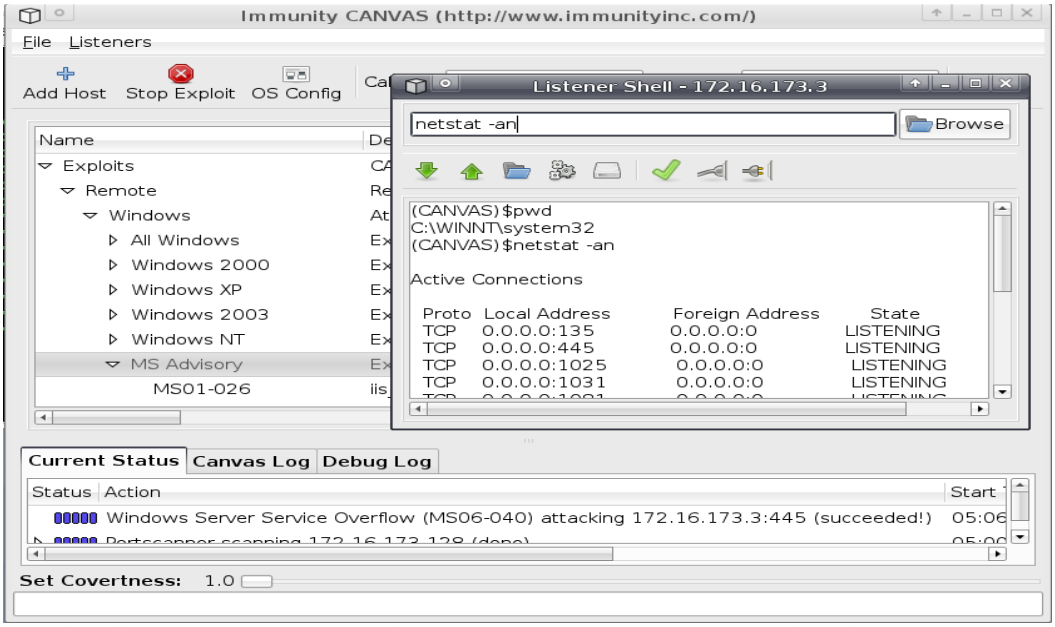
Pahalı olmasına rağmen yaygın olarak kullanılan en güçlü işleme aracı olarak kabul edilir. Şekil.4.2.2.2.1.'de yer alan Core Impact düzenli güncellenen veritabanı sayesinde profesyonel exploitler yaparak diğer makinalara kurduğu tünel sayesinde onları rahatlıkla exploit edebilir.



Şekil.4.2.2.2.1. Core Impact

4.2.2.3 Immunıty canvas

Şekil.4.2.2.3.1.'de yer alan Immunity Canvas Ticari bir araçtır. 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 kullanıcıya sunulur.



Şekil.4.2.2.3.1. Immunity Canvas

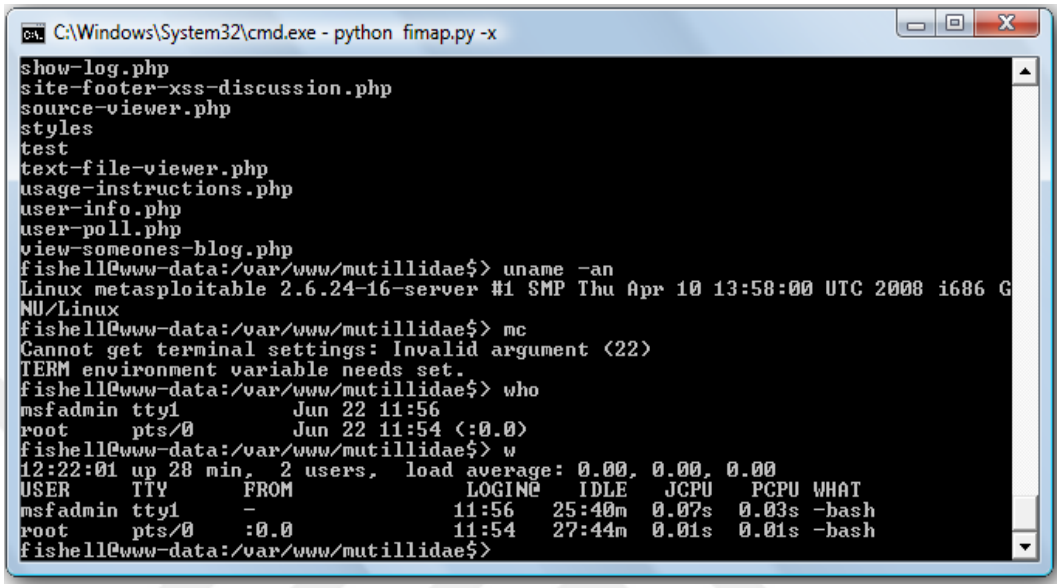
4.2.2.4 Sqlmap

SQL injection'ları tespit eden ve kusurları istismar ederek uç Veritabanı sunucularına erişimi sağlayan açık kaynaklı penetrasyon aracıdır. Şekil.4.2.2.4.1.'de örneği gösterilen SqlMap Out of band yoluyla işletim komutları DB'den veri getirmekte hatta temel dosya sistemine erişim sağlamaktadır

Şekil.4.2.2.4.1. SqlMap

4.2.2.5 Fimap

Şekil.4.2.2.5.1.'de yer alan Fimap bir python aracıdır. Bu araç, bulur, hazırlar, denetimi yapar, istismar eder ve webapps'lerdeki bug'ları bulur. Sqlmap'e benzer, farkı LFI / RFI bugları bulmasıdır.



Şekil.4.2.2.5.1. 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 [10]. Parola(şifre) kırma yöntemleri

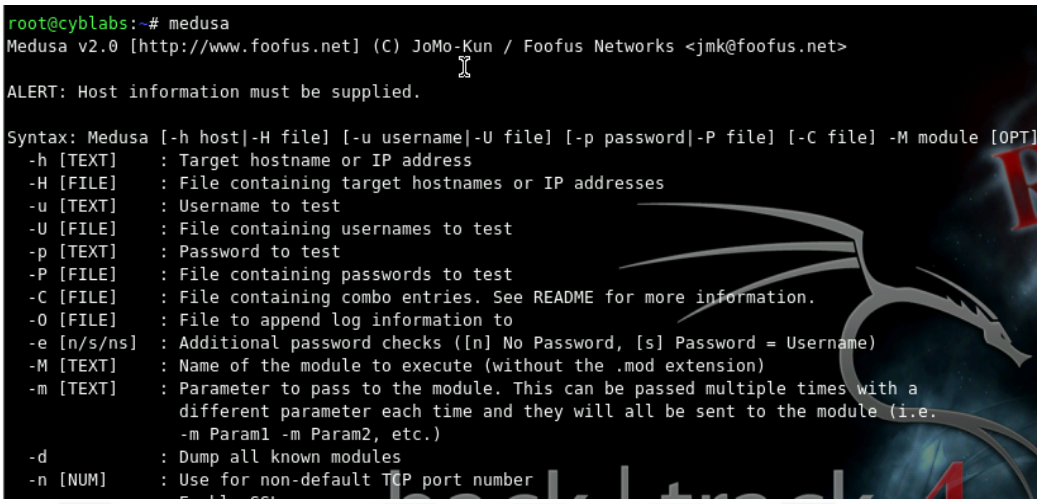
- Online parola(şifre) kırma (Aktif)
- Offline parola(şifre) kırma (Pasif)

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. Farklı portlarda çalışan servisler için port ayarı yapılabilir.

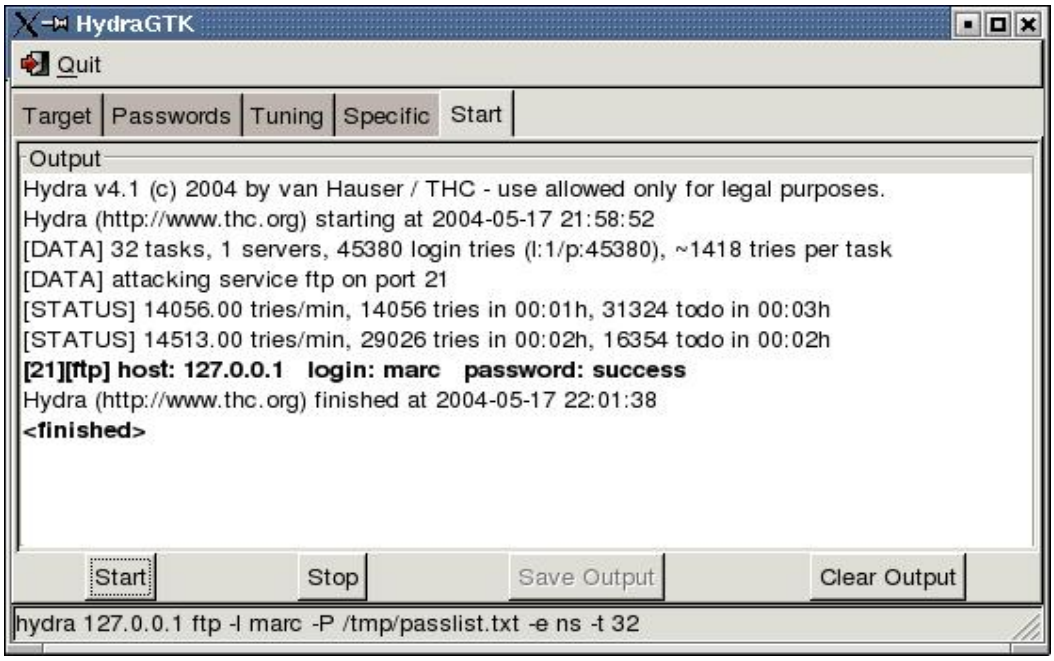
Paralel saldırı düzenleme seçeneği vardır. Ağ bağlantısına ve servisin durumuna göre hızı değişmektedir. Şekil.4.2.3.1.1.'de Medusa gösterilmektedir.



Şekil.4.2.3.1.1. Medusa [10]

4.2.3.2 Hydra

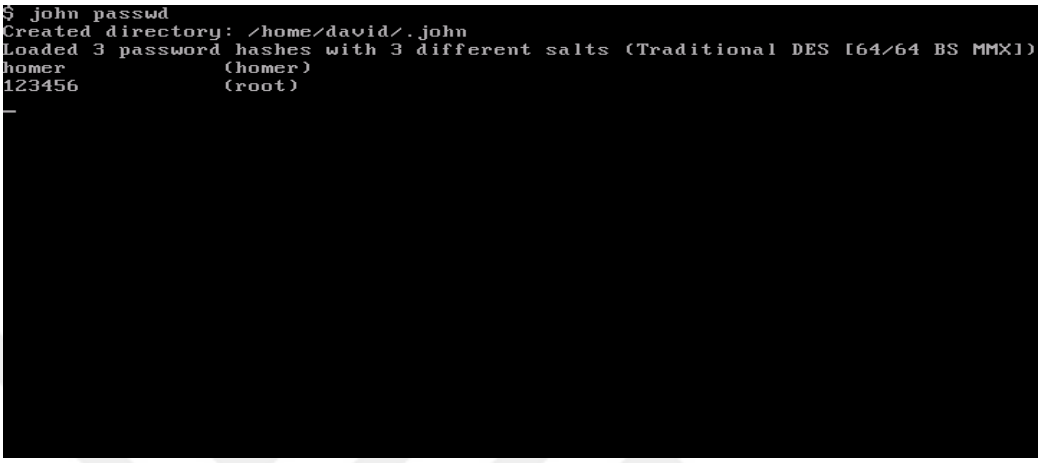
Şekil.4.2.3.2.1.'de yer alan Hydra, paralel ağ servisleri parola denetim(kırma) aracıdır. Konsol ve grafik arabirimden çalıştırılabilir. Hesap kitleme riski vardır. 30'dan fazla protokole karşı (telnet, ftp, http, https, smb vb.) brute force ataklarda kullanılır.



Şekil.4.2.3.2.1. Hydra

4.2.3.3 John the ripper

Şekil.4.2.3.3.1.'de gösterilen John The Ripper, pasif şifre kırma(denetim) aracıdır. Bilgi toplama vs sonrası ele geçirilen hashlenmiş parola dosyalarını kırmak için kullanılır. Yeni nesil Linux parolaları (Sha512 kullanılmış) JTR kırmak için ufak bir yama gerekmektedir.



Şekil.4.2.3.3.1. John The Ripper

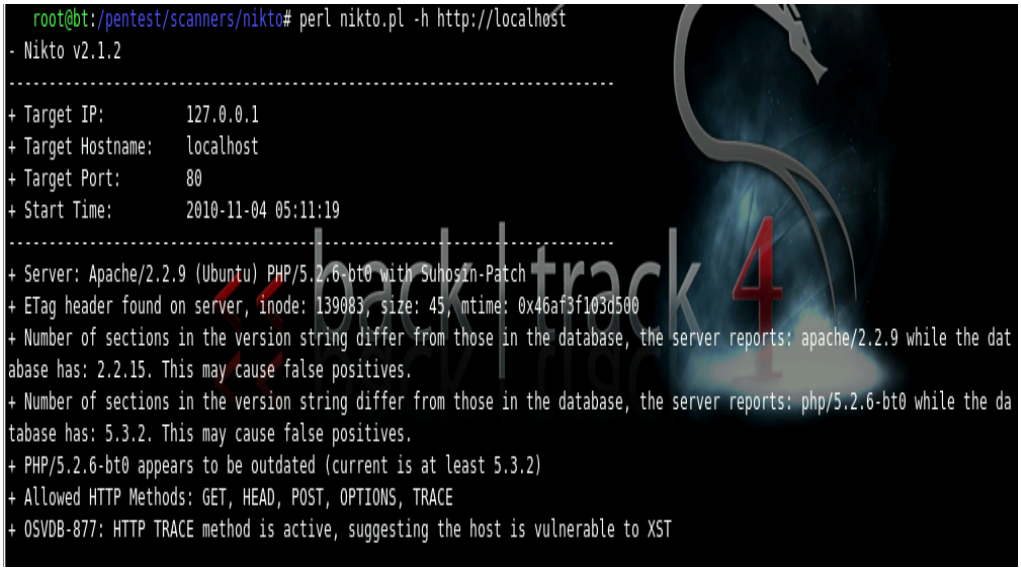
4.2.4 Web uygulama güvenlik testleri ve kullanılan temel araçlar

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 [11].

Gartner'a göre zafiyetlerin %75'i web uygulamalarında, güvenlik için harcanan paranın %90 ağ güvenliği üzerine olmaktadır.

4.2.4.1 Nikto

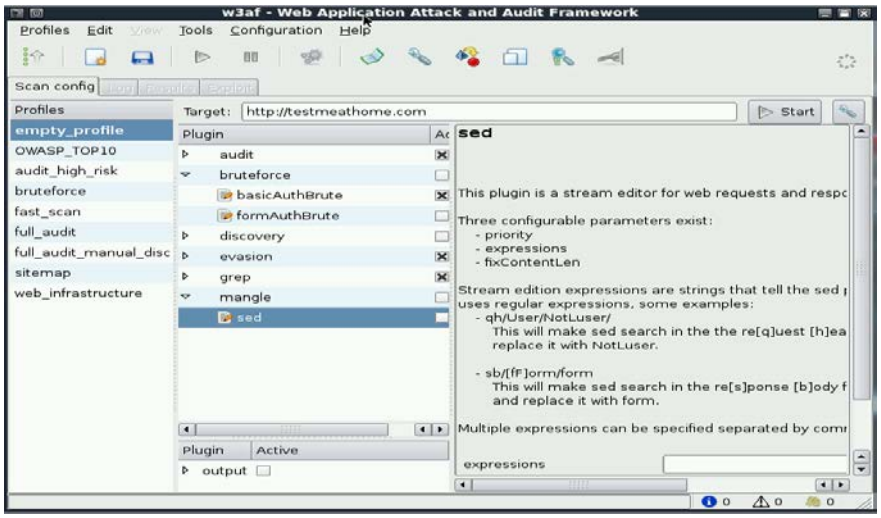
Şekil.4.2.4.1.1'de yer alan Nikto, statik web açıklık tarayıcısıdır. Aynı zamanda ilk web açıklık tarayıcılarındandır. Güvenlik açıklığı barındıran web sunucu yazılımları, test, dev. gibi yanlışlıkla unutulmuş dosyaları, yapılandırma hatalarını bulmak için kullanılır. Nessus entegrasyonu vardır. Günümüz uygulamaları için yeterli değildir.



Şekil.4.2.4.1.1 Nikto

4.2.4.2 W3af

Web aplikasyonu açıklıklarını bulmada son derece popüler, güçlü ve esnek bir araçtır. Kullanımı kolay bir ara yüze sahiptir. Birçok web değerlendirme özellikleriyle istismar eklentilerinin gelişiminde kullanılmaktadır. Şekil.4.2.4.2.1.'de örnek bir W3AF yer almaktadır.



Şekil.4.2.4.2.1. W3AF

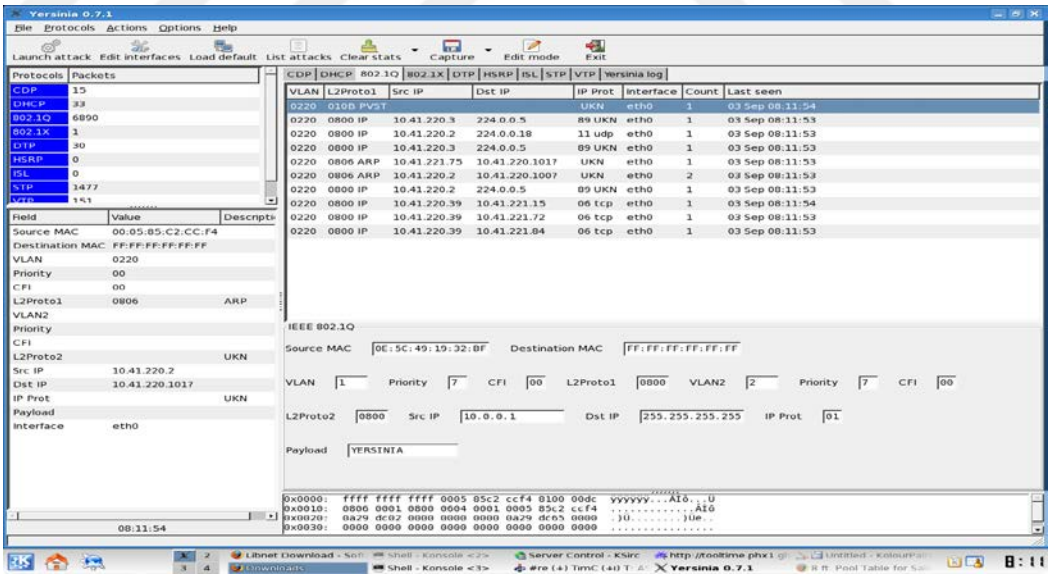
4.2.5 Yerel ağ protokolleri güvenlik testleri süreci ve kullanılan temel araçlar

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 [12].

4.2.5.1 Yersinia

Şekil.4.2.5.1.1.’de yer alan Yersinia ile birlikte kullanılan protokoller;

- 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)



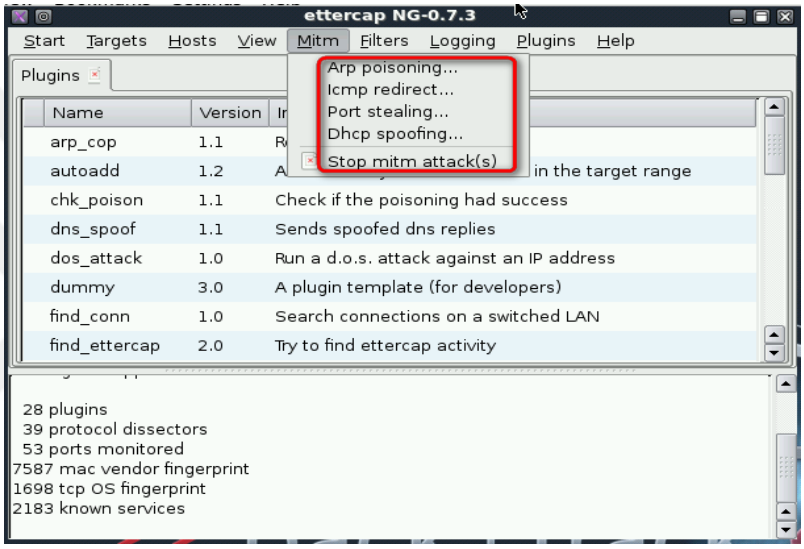
Şekil.4.2.5.1.1. Yersinia

4.2.5.2 Ettercap

Şekil.4.2.5.2.1.'de gösterilen Ettercap yerel ağlarda araya girme, bilgi çalma ve dos yapmak için kullanılan gelişmiş bir araçtır. MITM için çeşitli yöntemler kullanır.

Bu yöntemler;

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



Şekil.4.2.5.2.1. Ettercap

4.3 Zafiyet Tespit Araçlarının Artıları/Eksileri

Bu araçlar her zaman kesin sonuç vermemektedir. 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 alınmayacağı bilinmelidir..

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 yol olacaktır. Aşağıda bu yöntemler anlatılmıştır [13].

4.4.1.1. 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 araştırılır.

4.4.1.2. Sistem zayıflık incelemesi

Ağ ve sistemlerde bulunan potansiyel zayıflıklar araştırılır. 1. Adımda elde edilen bilgiler doğrultusunda potansiyel zayıflık araştırmaları ve saldırı planı geliştirilir. Potansiyel ağ altyapısı zayıflıkları ve eksiklikleri tespit edilir.

4.4.1.3. Zayıflık değerlendirmesi

Ağ haritası çıkarılır ve 2. Adımdaki tüm bileşenlerde bulunan zayıflıklar değerlendirilir. Hedef analizi sonrası hangi bileşenlere, sistemlere hangi protokollerle saldırılacağı belirlenir.

4.4.1.4. Araç analizi

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

4.4.1.5. Penetrasyon saldırıları

4.Adımda belirlenen araçlar ve 3. Adımda belirlenen saldırı senaryosu kullanılarak penetrasyon saldırıları düzenlenir. Bu saldırılar sonucu başarılı olanlar sınıflandırılır.

4.4.1.6. Zayıflık analizi

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

4.4.1.7. Geri bildirim süreci

Sistem güvenlik veritabanı, zayıflık veritabanı ve araçlar düzenlenerek raporlama aşamasına geçilir.

4.4.2 Bulgu önem dereceleri

Ağ ve sistemlerde bulunabilecek riskler çeşitli kategorilerde sınıflandırılır. Aşağıda bu risk sınıflandırmaları 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 [14].

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 gerekmektedir.

5. YÖNTEM VE METOD

Son olarak yukarıdaki bilgileri özet bir tabloda toparlanıp zayıflıklar listelenmiştir. Daha sonra da bu zayıflıkların giderilmesi adına çözüm önerileri uygulanmıştır. Sonuç olarak uygulanan çözümün söz konusu zayıflığı ortadan kaldırdığı görüldü.

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.5.1. İlk düzey 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.5.2. İkinci düzey bulgu önem derecesi

Unutmamak gerekir ki, bu fonksiyonel bir test değildir. Pentest'te amacınız sistemde güvenlik açıkları bulmaktır. Aşağıda bazı genel test durumları bulunmaktadır ve tüm uygulamalar için geçerli olmayabilir.

Öncelikle web uygulamasının, web sitesinde kullanılan iletişim formlarında spam saldırılarını tanımlayıp barındırabildiği kontrol edilmelidir.Proxy sunucusu - Ağ trafiğinin proxy uygulamaları tarafından izlenip araştırmadığını kontrol edilmelidir. Proxy sunucusu, bilgisayar korsanlarının ağın iç ayrıntılarını almasını ve böylece sistemi dış saldırılardan korumasını zorlaştırır.

Spam e-posta filtreleri - Gelen ve giden e-posta trafiğinin filtrelenip filtrelenmediğini ve istenmeyen e-postaların engellendiği doğrulanmalıdır. Birçok e-posta istemcisi, ihtiyaçlarımıza göre yapılandırılması gereken yapılandırılmamış spam filtrelerine sahiptir. Bu yapılandırma kuralları e-posta başlıklarına, konudan veya belge içinde uygulanabilir.

Güvenlik Duvarı - Tüm ağın veya bilgisayarların Güvenlik Duvarı ile korunmasını sağlanmalıdır. Bir Güvenlik Duvarı, sisteme yetkisiz erişimi engellemek için bir yazılım veya donanım olabilir. Güvenlik Duvarı, iznimiz olmadan ağ dışından veri göndermeyi engelleyebilir.

Tüm sunucular, masaüstü sistemler, yazıcılar ve ağ aygıtları kullanılmalıdır.

Tüm kullanıcı adları ve şifrelerin şifrelendiğini bununla birlikte https gibi güvenli bir bağlantı üzerinden aktarıldığı doğrulanmalıdır.

Web sitesi çerezlerinde depolanan bilgileri doğrulanmalıdır. Bu bilgiler okunabilir biçimde olmamalıdır.

Düzeltmenin çalışıp çalışmadığını kontrol etmek için daha önce bulunan güvenlik açıklarını doğrulanmalıdır.

Ağda açık bağlantının olmadığı doğrulanmalıdır.

Tüm mobil cihazlar doğrulanmalıdır.

WIFI güvenliği doğrulanmalıdır.

Tablo 5.1 de yer alan tüm HTTP yöntemlerini doğrulanmalıdır. PUT ve Delete yöntemleri web sunucusunda etkinleştirilmemelidir.

Tablo 5.1. 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

Parolanın gereken standartları karşıladığı doğrulanmalıdır. Parola, en az bir sayı ve bir özel karakter içeren en az 8 karakter uzunluğunda olmalıdır.

Kullanıcı adı “admin” veya benzeri isimlerde seçilmemelidir.

Başarısız birkaç giriş girişimi üzerine Uygulama giriş sayfası kilitlenmelidir.

Hata mesajları genel olmalı ve "Geçersiz kullanıcı adı" veya "Geçersiz şifre" gibi belirli hata ayrıntılarını belirtmemelidir.

Özel karakterlerin, HTML etiketlerinin ve komut dosyalarının bir giriş değeri olarak düzgün şekilde işlenip işlenmediğini doğrulanmalıdır.

Dahili sistem bilgileri herhangi bir hata veya uyarı mesajında gösterilmemelidir.

Web sayfası çökmesi durumunda son kullanıcıya özel hata mesajları gösterilmelidir.

Kayıt defteri girdilerinin kullanımını doğrulanmalıdır. Hassas bilgiler kayıt altına alınmamalıdır.

Tüm dosyalar sunucuya yüklenmeden önce kontrol edilmelidir.

Hassas veriler, web uygulamasının farklı dahili modülleri ile iletişim halindeyken URL'lerde iletilmemelidir.

Sistemde herhangi bir sabit kodlanmış kullanıcı adı veya şifre bulunmamalıdır.

Tüm girdi alanlarını boşluklu ve boşluksuz uzun girdi dizisi ile doğrulanmalıdır.

Şifre sıfırlama işlevselliğinin güvenli olup olmadığını doğrulanmalıdır.

SQL Enjeksiyon başvurusu doğrulanmalıdır.

Önemli giriş doğrulamaları, istemci tarafında JavaScript denetimleri yerine sunucu tarafında yapılmalıdır.

Sistemdeki kritik kaynaklar sadece yetkili kişiler ve servisler tarafından kullanılabilmelidir.

Tüm erişim günlükleri uygun erişim izinleriyle korunmalıdır.

Oturumu kapattıldığında kullanıcı oturumunun sona erdiğini doğrulanmalıdır.

Sunucudaki dizine gözatmanın devre dışı olduğunu doğrulayın.

Tüm uygulamaların ve veritabanı sürümlerinin güncel olduğunu doğrulanmalıdır.

Web uygulamasının istenmeyen herhangi bir bilgi göstermediğini kontrol etmek için URL manipülasyonu kontrol edilmelidir.

Bellek sızıntısını ve arabellek taşmasını doğrulanmalıdır.

Trojan saldırılarını bulmak için gelen ağ trafiğinin taranıp taranmadığını doğrulanmalıdır.

Sistemin Brute Force Attacks'den güvenli olup olmadığını kontrol edilmelidir.

Sistem veya şebekenin DoS (servis reddini) saldırılarından korunup korunmadığını doğrulanmalıdır. Hacker, hedef sistemdeki hangi kaynakların aşırı yüklenerek yasal isteklere karşı hizmet reddine yol açtığı için sürekli istekleri olan ağ veya tek bir bilgisayarı hedefleyebilir.

HTML komut dosyası enjeksiyon saldırıları için uygulama belirlenmelidir.

COM ve ActiveX saldırılarına karşı tedbir alınmalıdır.

Sistemi parodi saldırılarına karşı doğrulanmalıdır. Spoofing birden çok türde olabilir. IP adresi sızdırma, e-posta kimliği sızdırma, ARP sızdırma, yönlendirici sızdırma, arayan kimliği sızdırma, dosya paylaşım ağlarının zehirlenmesi, GPS sızdırma bu türlere örnek olabilir.

Kontrolsüz biçim dizesi saldırısı olup olmadığını kontrol edilmelidir.

XML enjeksiyon saldırısını doğrulanmalıdır. Bu yöntem uygulamanın mantığını değiştirmek için kullanılır.

Sistem Kanonikleştirme saldırılarına karşı doğrulanmalıdır.

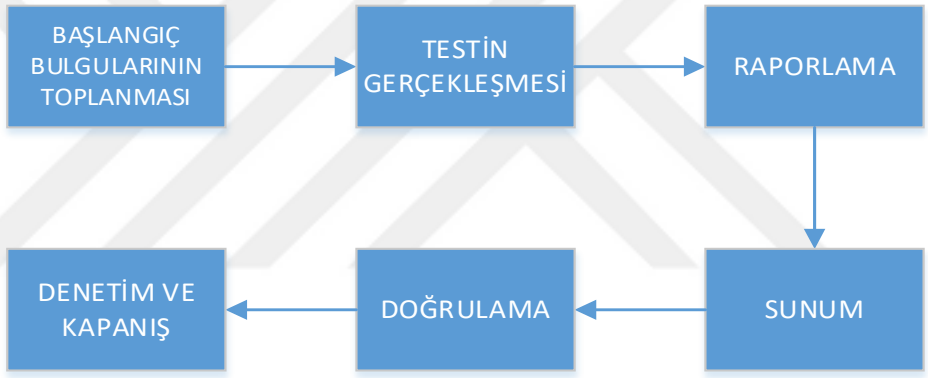
Hata sayfalarında bilgisayar korsanının sisteme girmesine yardımcı olabilecek herhangi bir bilgi gösterilip gösterilmediği kontrol edilmelidir.

Sistemdeki gizli dosyalarda şifre gibi kritik bilgilerin depolanıp depolanmadığını doğrulanmalıdır.

Uygulamanın, gerekli olandan daha fazla veri döndürüp yedeklemediğini doğrulanmalıdır.

Yukarıdaki yöntemler Pentest'i kullanmaya başlamak için temel test senaryolarıdır. Elle veya otomasyon araçlarıyla yapılabilen yüzlerce gelişmiş penetrasyon yöntemi vardır.

Penetrasyon testinin EPC (Event Process Chain) diyagramına göre yaşam döngüsü Şekil.5.3 de gösterilmiştir.



Şekil.5.3. Penetrasyon testinin EPC (Event Process Chain) diyagramına göre yaşam döngüsü

6. SONUÇ ve GELECEK ÇALIŞMALAR

Sonuç olarak, yapılan tüm araştırmalar ve testler verinin ve varlıkların korunmasının önemini gözler önüne sermektedir. 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 uygulanmak suretiyle tehdit bertaraf edilmiştir. Bu çalışma farklı kurumlar için de rahatlıkla planlanabilmektedir.

Hali hazırda çalışmış olduğum kurumumda (İspark A.Ş.) her yıl düzenli olarak bu testler yapılmaktadır. Özellikle Metasploit ve Coreimpact yöntemlerini kullanarak kullanıcı bilgisayarlarındaki zafiyetler ve sistemde oluşturduğu etkisini görebilmekteyiz. İlave olarak da çeşitli güvenlik firmalarının inhouse denilen yerel yazılımlarından da istifade ederek güvenlik seviyemizi üst seviyede tutmaya çalışmaktayız. Aynı yöntem yeni başlayan ve zamanla yaygınlaşacak, tüm İspark otoparklarının İstanbul Kart ile çalışmaya başlamasıyla arttırarak devam edecektir. 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 ihtimalleri tespit ediliyor olacaktır. Daha sonra da bu ihtimaller üzerinden gerekli tedbirleri alarak hizmete başlamış ve sonrasında sahadaki uygulamaya göre güvenlik tedbirlerimizi sık sık tekrarlamış olacağız. 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. Yine aynı minvalde oluşan büyük verinin korunması adına yeni test araçları üretilmeye devam edilecektir.

KAYNAKLAR

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

[2] Oksman V., (2010), "The mobile phone: A medium in itself", "VTT Publications 737", Elektronik Kitap

[3] G. Canbek, Ş. Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9(3):69-72.

[4] G. Canbek, Ş. Sağıroğlu, "Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi 23 (1-2) 1 - 12 (2007).

[5] TÜBİTAK, Bilgem, "UEKAE BGYS-0001 Bilgi Güvenliği Yönetim Sistemi Kurulumu".

[6] M. Gülmüş, "Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği ", Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, 2010

[7] Karabulut, Y.E. (2013). Penetrasyon Testi Nedir?. 06.07.2016, http://www.karabulut.co/penetrasyon-bilgi-toplama/.

[8] Işık, O.C. (24 Ocak 2015). Penetrasyon Testleri. 06.07.2016, www.networkpentest.net.

[9] Önal, H. (2010). Güvenlik Testlerinde Açık Kodlu Araçların Kullanımı. Bilgi Güvenliği Akademisi. Erişim tarihi A04.07.2016, http://www.bga.com.tr/.

[10] Weidman, Georgia (2014). Penetration Testing. A Hands-On Introduction to Hacking

[11] Isaca, Cisa Review Manual 2009, Isaca Press, Rolling Meadows, 2009.

[12] DeNardis L., The History of Information Security: A coprehensive handbook, Elsevier, 2007.

[13] Başaranoğlu E., Aralık 2014, Sistem ve Ağ Güvenliğine Yönelik Saldırı Türleri, Erişim Tarihi 20.06.2017, http://www.siberportal.org

[14] Başaranoğlu E., Temmuz 2015, Kurumsal Ağlarda Etki Alanı Sızma Testi Metodolojisi, Erişim Tarihi 21.06.2017, http://www.siberportal.org

ÖZGEÇMİŞ

Adı Soyadı : Ömer Faruk KAYA

Doğum Yeri ve Yılı : Trabzon 25.05.1982

Medeni Hali : Evli

Yabancı Dili : İngilizce

E-posta : omerfaruk.kaya@ispark.istanbul

Eğitim Durumu

Lise : Trabzon Lisesi, 1997

Lisans : Işık Üniversitesi, Bilgisayar Mühendisliği, 2001

Yüksek Lisans : İstanbul Ticaret Üniversitesi, Siber Güvenlik, 2015

Mesleki Deneyim

İştirakler Daire Başkalığı,
Bilgi İşlem Uzmanı 2009-2011

İSPARK A.Ş.
Bilgi İşlem Şefi 2011-2015

İSPARK A.Ş.
Ar-Ge Müdürü 2015-2017

İSPARK A.Ş.
Avrupa Yakası Otopark İşletmeleri Müdürü 2017-…

Yayınları