İZMİR KÂTİP ÇELEBİ ÜNİVERSİTESİ
2010
FEN BİLİMLERİ ENSTİTÜSÜ

Siber Güvenlik Alanında Sosyal Mühendislik Metodoloji Türleri ve Siber Saldırı Senaryolarına Yönelik İnceleme ve Uygulama Örneklemeleri

Yazılım Mühendisliği Ana Bilim Dalı

Tezsiz Yüksek Lisans Bitirme Projesi

Fethi ÇOBAN

ORCID 0000-0003-2785-6901

Proje Danışmanı: Prof. Dr. Femin YALÇIN KÜÇÜKBAYRAK

Ocak 2023

İzmir Kâtip Çelebi Üniversitesi Fen Bilimleri Enstitüsü öğrencisi **Fethi ÇOBAN** tarafından hazırlanan **Projenin Türkçe Başlığı** başlıklı bu çalışma tarafımızca okunmuş olup, yapılan savunma sınavı sonucunda kapsam ve nitelik açısından başarılı bulunarak jürimiz tarafından YÜKSEK LİSANS BİTİRME PROJESİ olarak kabul edilmiştir.

ONAYLAYANLAR:

Proje Danışmanı: **Prof. Dr. Femin YALÇIN KÜÇÜKBAYRAK**
İzmir Kâtip Çelebi Üniversitesi

Yazarlık Beyanı

Ben, **Fethi ÇOBAN**, başlığı **Siber Güvenlik Alanında Sosyal Mühendislik Metodoloji Türleri ve Siber Saldırı Senaryolarına Yönelik İnceleme ve Uygulama Örneklemeleri** olan bu projemin ve projenin içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu projenin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Projenin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Kayda değer yardım aldığım bütün kaynaklara teşekkür ettim.
- Projede başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

Tarih: 15.01.2023

Siber Güvenlik Alanında Sosyal Mühendislik Metodoloji Türleri ve Siber Saldırı Senaryolarına Yönelik İnceleme ve Uygulama Örneklemeleri

Öz

Günümüz döneminde hayatlarımızın hemen hemen her alanında sosyal, eğitim ve iş hayatında internetin yaygınlaşması ile tablet, bilgisayar, serverlar, cep telefonları ve network ağına bağlanabilen birçok cihazların ağlar üzerinden birbirlerine bağlanması, veri ihlalleri ve siber saldırılara sebebiyet vermektedir. Siber alanlar arttıkça, veri ihlalleri de önem kazanmaya başlamıştır. Bu çalışmada siber suç türleri, çeşitleri, amaçları ve zararlı yazılımlar ile birlikte kullanılan araçlar ayrıntılı bir şekilde incelenmiş ve bunlara karşı alınacak önlemler projede örneklemelerle belirtilmiştir. Bunun yanı sıra gelişmiş siber saldırılara örnek verilmiş ve bilgi güvenliği için yapılması gerekenlere bu projede yer verilmiştir. Ayrıca teknolojik olarak ne gibi tedbirlerin alınması gerektiğine de açıklık getirilmiştir. Hangi tedbir alınırsa alınsın en zayıf halka olan insanın, eğitim ile olası zararları en aza indirebileceği değerlendirilmektedir.

Anahtar Sözcükler: Siber alanlar, siber saldırı, siber suçlar, server, teknoloji

Types of Social Engineering Methodology in the Field of Cyber Security, Analysis and Application Examples for Cyber Attack Scenarios

Abstract

In almost every area of our lives in today's era of social, educational, and business life with the popularization of the internet, tablet computers, servers, mobile phones and the network via the network connected to each other many devices that can connect to the network, and data breaches caused by cyber attacks. As cyber areas increase, data breaches have also started to gain importance. In this study, the types, types, purposes of cybercrime and the tools used together with the malicious software were investigated in detail and the measures to be taken against them were indicated with examples in the project. In addition, examples of advanced cyber attacks have been given and what needs to be done for information security has been included in this project. In addition, it was explained what kind of technological measures should be taken. No matter what measures are taken, it has been emphasized that the person who is the weakest link can minimize the possible damages with education.

Keywords: Cyber areas, cyber attacks, cybercrime, server, technological measures

Proje çalışmasına katkılarından dolayı Proje Danışmanım Prof. Dr. Femin YALÇIN KÜÇÜKBAYRAK'a teşekkür ederim.

İçindekiler

Şekiller Listesi

Kısaltmalar Listesi

BGYS	Bilgi Güvenliği Yönetim Sistemi
BTK	Bilgi Teknoloji Kurumu
CMD	Komut Satırı
CNAME	Kanonik Ad Kaydı
DHCP	Dinamik Ana Bilgisayar Yapılandırma Protokolü
DNS	Alan Adı Sistemi
DVD	Çok Amaçlı Sayısal Disk
EBA	Eğitim Bilişim Ağı
HDD	Hard Disk
HTTP	Hiper Metin Transfer Protokolü
IP	İnternet Protokolü
ISS	İnternet Servis Sağlayıcısı
MX	Posta Değiştirici Kaydı
NMAP	Güvenlik Tarayıcısı
ORCID	Tescilsiz Alfanümerik Kod
PLC	Programlanabilir Mantıksal Denetleyici
PN	Aktif Bilgi Toplama Parametresi
SNMP	Basit Ağ Yönetim Protokolü
SSD	Katı Hâl Sürücü
UDP	Kullanıcı Veri Bloğu İletişim Kuralları
URL	İnternet Adresi
TCP	IP Protokol Türü
TLS	Aktarım Katmanı Güvenliği
TXT	Metin Uzantılı Dosya Türü
Wi-Fi	Kablosuz Bağlantı Alanı

Semboller Listesi

-sA	Durum bilgisi veren tarama türü
-sF	Bit ayarlanmasıyla gerçekleştirilen tarama türü
-sl	Hedefe yönelik tarama türü
-sM	Paket filtreleyen güvenlik duvarlarını atlatılabilen tarama türü
-sN	Hiçbir bayrağın bulunmayacağı tarama türü
-sS	TCP portlarını taramanın en hızlı türü
-sT	TCP tarama türü
-sU	UDP taraması türü
-sW	Portların açık olma durumlarını gösteren tarama türü

Giriş

Bu çalışmada son zamanlarda ciddi derecede artış gösteren veri hırsızlığı ve siber saldırılar karşısında alınması gereken tedbirler ve bu tedbirlerin neler olduğu araştırılıp, incelenmiştir. Siber güvenlik neden önemlidir? Bir fidye yazılımından nasıl korunulur? Sosyal Mühendislik saldırısı nasıl tespit edilir? gibi sorular cevaplanarak projeye başlanmıştır. Kötü amaçlı yazılımların nasıl ortaya çıktığı ve kimlik avı saldırısına karşı nasıl hareket edilmesi gerektiği açıklanmıştır. Proje kapsamında siber uzay, siber güvenlik, siber suç gibi kavramlar, dünyada adından söz ettirmiş bilişim suçlarına konu olan olaylar ve siber tehditler incelenmiştir. Siber olayların nasıl gerçekleştirildiği detaylı olarak anlatılmıştır.

Birinci bölümde, genel kanı ve görüşler ile birlikte istatistiki bilgilere yer verilmiştir. Projenin bu kısmında internet kullanım oranlarındaki artış ile dünya çapında yankı bulmuş veri ihlallerine yer verilmiştir. İkinci bölümde, Siber güvenlik nedir? Siber güvenlik neden önemlidir? Siber güvenlik senaryolarının neler olduğu açıklanmıştır. Üçüncü bölümde; siber suçların türlerine göre sınıflandırılması, siber suçların sebepleri, siber saldırıları kimlerin gerçekleştirdiği ve bu saldırıların türlerine yer verilmiştir. Ayrıca bu kısımda siber taciz, terörizm ve vandalizm hakkındaki kavramlara yer verilmiştir. Dördüncü bölümde, kimlik avı saldırısının tanımlanması ve bu saldırıları önleme konusu incelenmiştir. Bu saldırıların çeşitliliği ile hangi yöntem ve usulleri kullandıkları hakkında da bilgilere yer verilmiştir. Beşinci bölümde; kötü amaçlı yazılım olan virüsler, solucanlar, truva atları, fidye yazılımları ve casus yazılımlara değinilmiş, sistemde bu zararlı yazılımlar mevcut ise bu konuda nelerin yapılması gerektiği anlatılmıştır. Altıncı bölümde, Sosyal Mühendislik Saldırıları anlatılmıştır. Bu saldırıların gerçekleştirme şekli ve bunlara karşı alınacak tedbirler konu edinilmiştir. Yedinci bölümde; siber atakları meydana getirmek için hangi tarama araçlarının kullanıldığı ve bu tarama sonucu uygulanacak ataklar gösterilmiştir.

İnternet, insanların sosyalleşerek zaman geçirebileceği "mükemmel" bir hale gelirken, aynı zamanda siber suçlulara da büyük fırsatlar sunmaktadır. Suçlular, tüm alanların dijitalleşmesiyle bu duruma uyum sağlayarak ve dijital ortama geçmişlerdir. İnternet

aracılığıyla ulaşılan programların alışveriş, bankacılık, yemek siparişi vb. faaliyetler için kullanıldığını, tüm bu bilgilerin dijital ortamda saklandığını, her şeyin buradan yönetildiğini kavramaları çok hızlı şekilde gerçekleşmiştir. Milyarlarca dolarlık onlarca çeşitli para birimi her gün internet üzerinden dijital olarak hareket etmekte ve bu suçlular için büyük bir cazibe merkezi haline gelmiş ve suç işlemek için alternatif bir yol haline gelmektedir. Artık para çalmak, soygun yapmak bankaya gitmek yerine internet üzerinden kolayca yapılmaktadır. Veriyi korumak teknolojik unsurlarla mümkün olsa da harcanan paralar kimi zaman da veriyi korumada etkili olamamıştır. Günümüzde teknolojinin sağladığı savunma mekanizmaları çoğunlukla yapay zekâ ile donatılsa da en zayıf halka olan insan faktörü alınan tüm önlemlerin önüne geçmektedir. Siber zorbalar artık gelişmiş duvarları ve cihazları aşmaya uğraşmaktansa insan faktörünün daha kolay bir hedef olduğuna karar vermişlerdir.

Tüm dünyada artan teknolojik ürünlerinin kullanımları ile beraber, internete bağlanma oranları, siber zafiyetlerin ve saldırıların artmasının temel nedenlerindendir. Bireysel kullanıcıların ve kurumsal kullanıcıların 2015-2020 yılında maruz kaldığı siber saldırılara yönelik hazırlanan istatistiklerin küçük bir bölümü incelenmiş, incelenen bu sonuçların ışığında aşağıdaki olayların meydana geldiği ve yine burada da insan faktörünün ne kadar önemli olduğu bir kez daha anlaşılmıştır.

- Yahoo, 3 milyar güvenliği ihlal edilmiş hesapla (Statista) tüm zamanların en büyük veri ihlali rekorunu kırmıştır.
- 2019 yılında First American Financial Corp. Bankacılık işlemleri, sosyal güvenlik numaraları ve daha fazlası dâhil olmak üzere çevrimiçi olarak 885 milyon kişi ile rekor kıran bir başka şirket olmuştur.
- 2019’ yılında Facebook, 2012 yılından beri 600 milyon kullanıcının, kullanıcı şifrelerini güvence altına almadığını itiraf etmiştir.
- 2019’ yılında Georgia Tech’in mevcut ve eski öğrenci, personel ve öğrenci adaylarının kişisel bilgilerine bir hacker tarafından merkezi bir veri tabanı üzerinden erişildi. 1.3 milyon kişi bu siber saldırıdan etkilendi. Saldırıya uğrayan veri tabanı; isimleri, adresleri, sosyal güvenlik numaralarını ve doğum tarihlerini içeriyordu.

- 2020’ Wawa adlı Amerikan hipermarket zincirinin, alışveriş siteleri üzerindeki açık nedeni ile 30 milyon Amerikalının ve 1 milyon yabancı müşterinin kart bilgileri DarkWeb üzerinden satışa sunuldu.
- 2020 yılında ünlü MGM Resorts 142 milyon adet misafir kayıtları ve kişisel verileri DarkWeb’te ortalama 2.500 dolar üzerinden satışa sunuldu.
- 2020 yılında Nintendeo oyun sektöründe hem de e-posta servislerinde kişisel verilerin yayılmasına neden oldu. Nisan ayında, oyun devi 160 bin kullanıcısının hesaplarının saldırı altında olduğunu duyurdu.
- 2021 yılında 533 milyon Facebook kullanıcısının kişisel bilgileri ve telefon numaraları düşük seviye hackerların yer aldığı bir forumda yayınlandı. Bu tarz veriler genellikle dark web'de ücret karşılığında satılıyor. Ancak forumda verilerin ücretsiz olarak yayınlanması dikkat çekti.
- 2021 yılında Linkedln adlı çevrim içi kariyer platformu büyük boyutta bir veri ihlali yaşandığını duyurdu. Saldırganlar, platformu kullanan 700 milyondan fazla kullanıcının verisini açığa çıkardı. Platformun toplam kullanıcı sayısı 756 milyon civarındadır.

Bu kadar büyük çapta veri ihlalleri ve siber saldırılar, küresel anlamda alınması gereken önlemlerin ve bu önlemler doğrultusundaki büyük yatırımların yapılması gerektiğini gözler önüne sermektedir. Ancak ne kadar önlem alınsa da ve yatırım yapılsa da insan faktörünün ve insanların farkındalıklarının artırılmasının çok önemli olduğu görülmektedir. Tüm bu durumlar ele alındığında kullanıcı sayıları, saldırı yöntemleri ve saldırı türleri, veri sızıntıları sonucunda ortaya çıkan zararlar gözlendiğinde önemli ölçüde maliyet artışı görülmektedir. Siber saldırganlar güvenlik duvarları ya da sistemleri aşmak yerine artık maliyet gerektirmeyen insan faktörü üzerinden hedeflerine ulaşmaya çalışmaktadır. Bu durumdan anlaşılıyor ki teknolojiye ne kadar yatırım yapılırsa yapılsın insan faktörü tüm güvenlik cihazlarının en tepesindedir. Bu sorunu ortadan kaldırmak için bireysel ve kurumsal kullanıcıların farkındalıklarını sağlamak amacıyla eğitimleri her geçen gün artırmak gerektiği değerlendirilmektedir. Bu araştırmalar ve anlatılanlar doğrultusunda elde edilen bulgular bizi en büyük zafiyetin insan faktörü olduğu sonucuna ulaştırmaktadır. İnsan faktörünün de bütün bu bilgilere sahip olması, geçmişte karşılaşılan tecrübelerden haberdar olmasının çok önemli olduğunu göstermektedir.

2 SİBER GÜVENLİK NEDİR VE NEDEN BU KADAR ÖNEMLİDİR?

2.1 Siber Güvenlik Nedir?

Bilgi güvenliği olarak da bilinen siber güvenlik, bilgisayar donanımlarını, sistemlerini, ağlarını, programlarını ve verileri siber saldırılara veya dijital saldırılara karşı koruma yolları anlamına gelmektedir. Bu nedenle siber güvenlik, bilgisayarları, bilgi teknolojisini, network ağlarını vb. koruyan her adımı ifade etmektedir. Etkili siber güvenlik adımları, siber saldırı risklerini azaltır ve sistemlerin, ağların ve teknolojilerin yetkisiz kullanımına karşı koruma ve güvenlik sağlar. Siber güvenlik, "Bilgi Güvenliği" teriminin bir parçasıdır.

Siber güvenlik olgusunu oluşturan faktörler şu şekilde incelenebilir. Bu faktörlerin başında İnsan gelmektedir. İnsanlar bir sistemin parçasıdır. 2019 yılında yapılan bir araştırmada, İnsan Faktörü raporuna göre yapılan siber saldırılarda saldırganlar, zararlı yazılım yüklemek, gizli bilgileri çalmak veya dolandırmak amacı doğrultusunda, çoğunlukla çalışan sistemlerin yerine insanları hedef almaktadır. Yapılan ihlallerin %99'unda insan faktörüne odaklanan saldırganlar sms, e-posta, sosyal medya ve bulut uygulamaları hedeflerine saldırmak için sosyal mühendisliği kullanmaktadır. E-postaların gerçeklerine çok benzeyen sahtelerini göndermek, kimlik bilgilerini ele geçirmeye çalışmak veya kötü amaçlı ekleri bulut uygulamalarına yüklemek, başarısız olma ihtimali yüksek maliyetli, zaman alıcı saldırıdan daha kolay ve çok daha avantajlıdır. Saldırıların önemli bir oranın insan hatalarından faydalanarak oltama e-postasındaki bir linke tıklama veya kötü amaçlı bir dosyayı açmak gibi insan etkileşimine bağlı olduğuna dikkat çekilmektedir. Güvenlik uzmanları, saldırılarda sosyal mühendisliğin öneminin çok fazla olduğunu ve güvenlik teknolojileri ve koruma seçenekleri ne kadar gelişirse gelişsin bu saldırıların devam edeceğini belirtmişlerdir. 2018'de gerçekleşen her dört kimlik avı e-postasından birinin Microsoft ürünleriyle bağlantılı olması da araştırmada öne çıkan önemli detaylardan birisidir.

İkinci bahsedilmesi gereken faktör süreçtir. Kuruluşların, hem denenmiş hem de başarılı olmuş siber saldırıları etkisiz hale getirebilmek için belirli birimlere sahip olması gerekmektedir. En üst seviyede bilgi güvenliği stratejisi ve politikaları, bu politikaları destekleyen süreç, prosedür ve talimatların organizasyon yapısına uygun olarak meydana gelmesi ve hayata geçirilmesi oldukça önemlidir. Tüm politika, süreç, prosedür ve talimatların tamamını açıklamak mümkün değildir, ancak siber güvenliğin sağlanması açısından bu tip bir yaklaşımın olaya özgü özel olarak oluşturulması gerekmektedir. Burada süreç ile kastedilen kısım, bir durumun kim tarafından ve ne şekilde ele alınması gerektiğinin incelenmesidir. Ayrıca bu süreçlerin sürekli olarak göz önünde bulundurulması, bu süreçlerin de bir olgunluk modeli üzerinden oluşturulması ve devamlı olarak geliştirilmesi gerekmektedir. Kurumsal bir operasyonu verimli ve doğru bir şekilde yürütebilmek için tanımlı ve önceden hazırlanmış süreçlere ihtiyaç vardır. Bu süreçler organize, etkili, tutarlı ve doğru bir şekilde yürütülmesi gereken olayın ve kişilerin hangi işleri nasıl yapacağına dair kendilerine yol gösteren haritalarıdır. Siber güvenlik alanında kuruluşların faaliyetlerini yürütebilmesi için gerekli olan süreçlerden bazıları şu şekilde sıralanabilir.

- Sürekli Güvenlik İzleme
- Siber Olay Yönetimi ve Müdahale
- Kimlik ve Erişim Yönetimi
- Log Yönetimi
- Çağrı Yönetimi
- Değişiklik Yönetimi
- Siber Tehdit ve İstihbarat Yönetimi
- Zafiyet Yönetimi
- Risk Yönetimi

2.2 Siber Güvenlik Neden Önemlidir?

Tüm Dünya; teknolojiye, geçmiş yıllarda olduğundan daha fazla bağımlı hale gelmiştir. Bu durum, dijital verilerin oluşturulmasında çok büyük bir artışa neden olmuştur. Veriler, bireyler, işletmeler, devlet kurumları vb. tarafından bilgisayarlarda depolanır ve günlük olarak bir ağ üzerinden diğer bilgisayarlara aktarılmaktadır.

Bilgisayarlar ve bağlı oldukları sistemlerde güvenlik açıkları bulunabilmektedir. Bunlar bir saldırgan tarafından istismar edilebilir ve bu da bir sistemin tamamen veya kısmen çökmesine yol açabilir. Bu nedenle siber güvenlik hayati önem taşımaktadır.

2010 yılının Haziran ayında ortaya çıkan bilgisayar solucanının hem yayılma biçimi hem de siyasi olarak kullanış şekli tüm Dünyada dikkat çekmiştir. Microsoft'un Windows tabanlı işletim sistemi üzerinden dağılan bu solucan, Siemens'in S7 300 PLC modüllerini hedef almıştır. Bu sistemler, ülkelerinin sanayisinin çok büyük bir kısmını oluşturan çeşitli sanayi işlemlerini otomatik olarak çalıştıran programlanabilir lojistik kontrol unsurlarını (PLC) denetlemektedir. Zararlı yazılım tarafından nükleer reaktörlerdeki basıncı kontrol ederek artırabilen, petrol boru hatlarının kontrol edilmesi ile aynı zamanda kapatabilen, sistem operatörlerine de her şeyin normal seviyede olduğu bilgisini vererek sıkıntıların son ana kadar anlaşılmamasına sebep olmuştur. Standart virüslerin aksine, sisteme girişi gerçekleştirmek için sahte güvenlik sertifikası kullanmıştır. Dünyanın en büyük şirketleri, Realtek'in güvenlik sertifikasını kullanmaktadır. Bu olay, sistemlere sızarak bir süre habersizce beklemesini ve sonra çalışmasını açıklamaktadır. Üstelik zararlı yazılımın işleyişini değerlendiren uzmanlar, bulaştığı sistemin yöneticileri tarafından haberdar olmadığı açıkları kullandığını görmüşlerdir. Bu açıklara "Zero Day" denilmektedir, bir sistemdeki ''Zero Day'' açığı, 200.000'den fazla bilgisayara bulaşmış ve 1.000 makinenin fiziksel olarak bozulmasına neden olmuştur.

İhlalden etkilenen ülkeler arasında İran (% 58,9) ve Endonezya (%18,23)'nın ilk sıralarda yer almıştır. Bu nedenle virüsün doğrudan bu ülkeleri hedef aldığı belirlenmiştir. Özellikle de nükleer santrallerinin zarar gördüğü İran'ı hedef aldığı tespit edilmiştir. Saldırılan ülkenin İran olması ve virüsün etkili olduğu zamanlarda İran'ın açıklama yapmadan nükleer faaliyetlerine ara vermek zorunda kalması nedeniyle, saldırının kimin organize ettiğinin tahmin edilmesi zor değildir. Fakat bunu kesin kanıtlarla ortaya koymak mümkün değildir.

2.3 Siber Güvenlik Senaryoları

Tüm teknolojik alanlarda siber güvenliğin kullanıldığı birkaç yaygın senaryo vardır. Bu senaryoların yansımaları her geçen gün artmaktadır. İşletmelerin sorunsuz çalışması için tüm dijital ihtiyaçlarını karşılayacak ve en son teknoloji güvenlik

ekipmanlarına sahip olunması şart hale gelmiştir. Bu ekipmanlar ile altyapısının 7/24 çalışır durumda olması önemlidir. Şirketlerin kuruluşların amaçlarını ve hedeflerini gerçekleştirmek için birlikte çalışan birçok sistem vardır. (Sunucular, güvenlik duvarları, switchler vb.) Dijitalleşme aynı zamanda bir kuruluşun ulaşılabilirliğini, sınırlarını genişleterek bağlantılarını ve çevresini artırmaktadır. Bu durum elbette bugün çok büyük bir avantajdır, ancak ilerleyen zamanlarda kuruluşa zarar verebilme ihtimalide vardır.

Üç adet bakış açısı dijitalleşmeyi ve bağlanabilirliği tanımlar:

● Kimlik : Kullanıcıların etkileşimde bulunabileceği bir özelliktir.

● Veri : Kullanıcı, işletme, sistem veya müşteri ile ilgili bilgilerdir.

● Ağ : Herkesin bağlı olduğu ve erişim seviyeleriyle kısıtlandığı bölümdür.

Bu üç bakış açısı, donanım, yazılım ve iş süreçleri aracılığıyla birbirine bağlıdır. Daha önce de belirtildiği gibi, bir yapı bu seviyeyi kontrol eden bir kullanıcının kimlik için geliştirilen erişim yoluyla verilerin oluşturması, görüntülemesi veya değiştirmesi gerekmektedir. Hem statik hem dinamik verilerin aynı anda güvenliğinin sağlanması gerekmektedir. İster fiziksel ister bulut ortamında, bu altyapının ağ çevresinin güvenliğinin de sağlanması gerekmektedir.

3 SİBER SALDIRILAR VE HACKERLER

İnternet başlangıçta savunma sanayi, büyük kuruluşlar ve araştırma topluluklarıyla sınırlıydı. Dolayısı ile siber suçun etkisi o zamanlar yok denilecek kadar azdı. İnternet 1996 yılından itibaren halka açık olarak kullanılmaya başlanmıştır. İnsanların hayatlarını kolaylaştırarak popüler hale gelmiştir. İnternet için grafik kullanıcı arayüzü çok basit bir şekilde tasarlanıp, kullanıcıların işlevlerini, kabiliyetlerini ve özelliklerini anlaması kolaylaştırılmıştır. Kullanıcılar, tarayıcılarındaki link köprülerine tıklayarak veya tarayıcıya URL'leri yazarak ulaşmak istedikleri verilere ulaşmaktadırlar. Verilere başka birinin erişimi olup olmadığını veya ulaştıkları verilerin bir saldırgan tarafından

izinsiz şekilde yönlendirilip kullanıldığının farkında değildiler. Siber suçların odağı olan internet yaygınlaştıkça ve büyüdükçe bir bilgisayara fiziksel olarak zarar vermek yerine, verilere müdahale ederek mali suçlar işlenmeye başlanılmıştır.

3.1 Siber Suçların Sınıflandırılması

Kurumlar, çalışanları ve müşterileri hakkında çok önemli veriler içeren büyük kapasiteli veri tabanı veya sunucu bulundurmaktadırlar. Siber suçlular için veri tabanları önemli veriler olduğu için bu kurumları hedef almaktadırlar. Bir siber suçlu, kuruluşun çalışanı veya dışarıdan herhangi birisi olabilir. Bu duruma göre siber suçları ikiye ayrılır;

3.1.1 İçeriden Bilgilendirme Saldırısı

Bir sisteme veya bilgisayar altyapısına erişimi olan birinin saldırısı, içeriden yapılan bir saldırı türüdür. Bu saldırganlar, hırs ve intikam gibi çeşitli nedenlerle saldırıyı gerçekleştirmektedir. İçeriden biri, güvenlik sisteminin altyapısının, politikalarının ve zayıflıklarının farkında olduğu için sisteme kolaylıkla saldırabilmektedir. Bu kişinin ayrıca kuruluşun ağına erişim yetkisi mevcuttur. Bu sebeple içeriden birinin bilgi çalması veya altyapıya zarar vermesi oldukça kolaydır. İçeriden biri, özellikle sisteme yeni pozisyonlar atandığında, genellikle saldırı için bir fırsat penceresi bulmaktadır. Örneğin, bir şirket yeni bir uygulama geliştirip çalışmaya başladığında, uygulamadaki verileri korumak için gerekli kontrollere ve politikalara sahip değildir. İçeriden bir kişi bu güvenlik zafiyetini, hedefini gerçekleştirmek için kullanır. Kurum içi güvenlik sistemleri dâhili olarak kullanılarak saldırıyı tespit edip aynı zamanda önleyebilmektedir.

3.1.2 Harici Saldırı

Kuruluşun içinden veya dışından kuruluşun ağına ve sistemlerine saldırmak için bir bilgisayar korsanı kiralandığında harici saldırılar ortaya çıkmaktadır. Bir sistemde mali ve itibar kayıplarına sebep olmak için harici saldırılar yapılmaktadır. Dışarıdan yapılan saldırı, içeriden yapılan ve yapılabilecek saldırılara kıyasla daha fazla planlamaya ve araştırmaya ihtiyaç duymaktadır. Her harici saldırı aşağıda sıralanan aşamalardan geçmektedir:

● Planlama

● Keşif

● Tarama

● Erişim Elde Etme

● Erişimi Sürdürme

Kuruluşun ağ yöneticisi, güvenlik duvarı günlüklerini devamlı kontrol etmelidir. Güvenlik açıklarını belirlemek için sistemleri ve ağı sürekli olarak taraması gerekmektedir. İçeriden saldırıların ve harici saldırıların yanında, iki tür siber saldırı daha vardır: Yapılandırılmış veya yapılandırılmamış saldırılar. Bu sınıflandırma, saldırganın deneyimine ve bilgisine dayanmaktadır. İnsanlar bu saldırıları dış saldırılar olarak sınıflandırmaktadır. Bir çalışan, kişisel kazanç sağlamak için kuruma yapılandırılmış saldırılar gerçekleştirir. Bu tür saldırılar genellikle rakip şirketler tarafından yapılmaktadır. Bunu, çalışanlarından birini rakip şirkete gönderip o şirketten bilgi toplamasını isteyerek gerçekleştirirler. Bu kurumsal casusluk olarak bilinmektedir.

3.2 Yapılandırılmamış Saldırılar

Önceden tanımlanmış bir nedeni olmaksızın amatör bir saldırgan tarafından gerçekleştirilen bir saldırı, yapılandırılmamış saldırı olarak sınıflandırılmaktadır. Bu saldırılar internette kolayca bulunabilen bir sızma aracı kullanılarak gerçekleştirilmektedir. Saldırgan bu aracı şirketin ağında kullanarak gerekli sızma işlemlerini gerçekleştirir.

3.3 Yapılandırılmış Saldırılar

Yapılandırılmış saldırı, hedefleri net olan deneyimli ve profesyonel biri tarafından dikkatlice planlanır ve yürütülür. Saldırganlar, saldırı tespit sistemi tarafından tespit edilmeden, hedef sisteme veya ağa erişmelerine yardımcı olan araçlara ve teknolojilere erişebilmektedir. Bir saldırgan, mevcut bir aracı belirli saldırı şekline uyacak şekilde değiştirmek için gerekli bilgiye sahiptir.

3.4 Siber Suçların Nedenleri

Bir saldırgan, çeşitli nedenlerle bir kuruluşun sistemine veya ağına erişmektedir. Siber suçların meydana gelmesinin yaygın nedenlerinden bazıları şunlardır:

3.4.1 Para

Saldırganlar, para kazanmanın daha kolay ve hızlı bir yolu olduğunu düşündüğü için siber suçlar işlemektedirler. Birinin hesap bilgilerini ifşa etmek ve kandırmak için kimlik avı sahtekârlığı yöntemini kullanmaktadırlar. Saldırgan, bu bilgileri, kurbanın hesabından kendi hesabına para aktarmak için kullanmaktadır.

3.4.2 İntikam

Bazı saldırganlar kişi, kuruluş, din veya hükümete karşı intikam almak için saldırı düzenlemektedirler. Mali ve fiziksel kayıplara neden olmak için bu saldırıyı gerçekleştirmek öncelikli amaçlarıdır. Bu saldırı biçimi ‘’Siber Terörizm’’ olarak adlandırılmaktadır.

3.4.3 Tanınma

Bazı saldırganlar popülerlik kazanmak, toplumda ün kazanmak için saldırılar gerçekleştirmektedir. Büyük kuruluşların sistemlerine ve ağlarına, kendilerine bir isim vermek için (anonimlik) saldırırlar. Siber suçlular, bilgisayarı ya da sistemi ele geçirdiklerinde (hack yaptıklarında) anonim kalmak isterler. Bu kişiler kendilerine takma isimler vererek ‘’t4cs1zkr4l’’ gibi bazı sitelerde kendilerine yer bulmaya veya başarı sırası kazanmaya çalışırlar. Bu anonimlik, saldırganları kişisel kazanç sağlamak için siber suç işlemeye teşvik etmektedir.

3.4.4 Siber casusluk

Bazı devletler, veri gizliliği yasasını görmezden gelmeyi ve vatandaşlarının yaptığı her şeyi izlemeyi seçebilirler. Bunu, siyasi veya ekonomik nedenlerin yanında istihdam sağlamak, kendi nam ve hesaplarına çalıştırmak için kullanırlar.

3.5 Siber Hacker Türleri

Bilgisayar korsanları yapıları gereği ağların ve bilgisayar sistemlerinin nasıl çalıştığını merak etmektedirler. Programlama ve kodlama konusunda yeteneklidirler. Becerilerini geliştirmek için ellerinden gelenin en iyisini yapmaktadırlar. Ayrıca bilgisayarı ve sistemleri ele geçirmek için kullanabilecekleri çeşitli araçlar ve teknolojiler hakkında bilgi sahibidirler. Bilgisayar korsanları genellikle işletim sistemlerine saldırdıkları için, farklı sistem türleri hakkında fazla bilgi edinmektedirler. Herhangi bir güvenlik açığını belirlemek için sistemde kendi yollarını bulmaktadırlar. Günümüzde "Hacker" denildiğinde herkesin aklına genellikle yıkıcı, kötü amaçlı bilgisayar saldırganları gelmektedir. Bu her zaman böyle değildir. Bilgisayar ve internet ile azıcık haşir neşir olan çoğu insanın kafasında oluşturduğu bu kavram doğru değildir. Hacker'ın kelime anlamı: "Bilgisayar korsanı" demektir. Bu korsanların da kendi içlerinde zararlı olanı ve zararsız olanları bulunmaktadır.

3.5.1 Beyaz Şapkalı Hackerler

Beyaz Şapkalı Hackerler, bilişim suçları işleyen kötü niyetli kişilerin kullanmış oldukları teknik ve yöntemleri iyi bir şekilde bilmektedirler. Siber korsanların eylemleri sırasında kullandıkları araçları ve yazılımları tanıyan, aynı bilgi ve beceriye sahiptirler. İyi niyetli siber güvenlik uzmanlarıdır. Bu kişilere ‘’Etik Hacker’’ veya ‘’Güvenlik Uzmanı’’ da denilmektedir. ‘’CEH’’ ya da tam ismiyle ‘’Certified Ethical Hacker’’ adı ile dünya çapında tanınmaktadırlar. Hacking becerilerini, savunma amaçlı kullanırlar. Danışmanlığını yaptığı kurum ve kuruluşların saldırıya uğramasını engellemeye çalışırlar. Bu saldırıları en az zararla atlatmalarını sağlarlar.

3.5.2 Siyah Şapkalı Hackerler

Bilgisayar korsanları olarak da bilinen siyah şapkalı korsanlar, sisteminize ve ağınıza erişmek, verilerinizi çalmak, değiştirmek veya yok etmek isteyen kötü niyetli saldırganlardır. Saldırıları için ortak hackleme uygulamaları kullanırlar. Kanunlara aykırı davranırlar ve suça eğilimlidirler. Hedeflerine göre beyaz şapka ile siyah şapka korsanını birbirinden ayırmak oldukça kolaydır.

3.5.3 Gri Şapkalı Hackerler

Kullandığı illegal yöntemlerle sistemin açıklarını bulan ancak bulduğu açıkları zararsız ve masum kullanıcılara zarar vermek için kullanmayan hacker sınıfıdır. Gri şapkalı hackerler buldukları açıklarla kullanıcılara zarar vermezler. Bunun yerine kendini o açığı kapatmaya ve kullanıcılar için tehdit olmaktan çıkarmaya çalışırlar. ‘’Gri Şapka’’ veya ‘’Gray Hat’’ kavramı ilk defa 1998 yılında ortaya çıkmıştır. Bir grup hacker bir sistemin açığını fark etmişlerdir. Ancak açığı kullanmak yerine şirkete bildirmeyi tercih etmişlerdir. Daha sonradan bir felsefe haline gelen gri şapkalı eylemler günümüzde dahi hala devam etmektedir.

3.5.4 Lamerler

Lamerler, deneyim ve bilgiden yoksun oldukları için bilgisayar korsanlığı dünyasındaki en tehlikeli kişiler olarak bilinmektedirler. İnternette bulunan herhangi bir kötü amaçlı aracın veya yazılımın ne için kullanıldığını bilmeden kullanmaktadırlar. Ağa veya sisteme verebilecekleri zarar hakkında hiçbir fikirleri yoktur. Bilgisayar korsanlığı dünyasındaki varlıklarını sürdürmek isteyen bilgisayarlara ve ağlara saldırırlar.

3.5.5 Yeşil Şapkalı Hackerler

Yeşil şapka bilgisayar korsanları da bilgisayar korsanlığı dünyasının amatörleridir. Ancak onlarla lamerler arasında bir fark vardır. Hackleme konusunda çok az bilgiye sahiptirler. Profesyonel bilgisayar korsanları olma konusunda tutkulu olduklarından, hacklemek için gerekli becerilerini geliştirmeye çalışmaktadırlar. Diğer bilgisayar korsanlarından ilham almakta ve saldırıları öğrenmek için onlarla iletişim halinde kalmaktadırlar.

3.5.6 Red Hat Hackerleri

Kartal gözü korsanları olarak da bilinen kırmızı şapkalı bilgisayar korsanları, beyaz şapka korsanları gibi çalışmaktadırlar. Siyah şapka bilgisayar korsanları tarafından gerçekleştirilen saldırılara karşı koymak için ellerinden geleni yaparlar. Aradaki fark, kırmızı şapka korsanlarının acımasız olmaları ve siyah şapka korsanlarının kullandığı ağı ve sistemi yok etmeleridir.

3.5.7 Devlet Destekli Hackerler

Farklı ülkelerden korsanlar kullanılmaktadır. Savunma sistemleri ile ilgili bilgileri elde etmek için diğer ülkelerin sistemlerine girmeleri hedeflenmektedir. Hükümetin maaşlı elemanlarıdır.

3.5.8 Hacktivist

Hacktivism (aktivivism), "hackleme" ve "aktivizm" kelimelerinin karışımından oluşmaktadır. İnsanların interneti genellikle siyasi veya sosyal nedenlerle kullandıkları belirlenmiştir. Bu insanlara bazen sosyal adalet savaşçıları denilmektedir. Hacktivizm ve aktivizm birbiriyle ilişkilidir. Bununla birlikte, bu saldırılar çoğunlukla dijital olarak yapılmamaktadır. Hacktivistler (bu çabalara katılan insanlar) genellikle finansal kazançlar peşinde değildirler. Bunun yerine bir tür açıklama yapma çabası içindedirler. Bilgisayar korsanlığının ardındaki asıl amaç açıklama yapma çabası için saldırmaktır. Sivil itaatsizlik yerine, internet mesajlarını tüm dünyaya yaymak, onlar için çok önemli bir araçtır.

3.6 Bilgisayar Korsanları Tarafından Kullanılan Genel Araçlar

Bilgisayar korsanları, mükemmel bir saldırı gerçekleştirmek için çok sayıda araç kullanır. Bu araçlar şu şekilde listelenmektedir:

3.6.1 Rootkit

Dosyaları, çalışan süreçleri veya sistem içindeki bilgileri işletim sisteminden gizleyerek varlığını hissettirmeden sürdüren programların bütününe verilen addır. Asıl amacı sistem üzerinde yayılmak değil bulunduğu sistem içinde varlığını gizlemektir. Bu durum tipine göre değişmekle birlikte genellikle erişim yetkisi dâhilinde sisteme kurabilecek rootkit'ler vardır. Güvenilir bir kaynaktan geldiğine inandığınız bir programı haddinden fazla yetki ile çalıştırmak (Ör: root veya root yetkili bir grubu üyesi) zararlı bir rootkit'in sisteme kurulmasına sebep olmaktadır.

3.6.2 Tuş kaydediciler (Keylogger)

Keylogger'lar, klavyede basılan her tuşu kaydedebilen araçlar olarak bilinmektedir. Keylogger'lar herhangi bir uygulamanın, uygulama programlama ara yüzüne gizlenir. Uygulamaya eriştiklerinde kullanıcı tarafından yapılan her tuş vuruşunu kaydetmektedirler. Kaydedilen tuş vuruşları, kullanıcı adları, şifreler, web sitesi URL'leri, açık uygulamalar vb. gibi hassas verileri bir dosyaya kaydederler. Tuş kaydediciler ayrıca, klavye kullanılarak yazılmaları şartıyla kredi kartı bilgilerini, cep telefonu numaralarını, e-posta uygulamalarına yazılan kişisel mesajları vb. kaydedebildikleri için oldukça tehlikelidir. Keylogger'lar, hedef bilgisayara truva atları gibi kötü amaçlı yazılımlar kullanılarak yerleştirilir.

3.6.3 Güvenlik Açığı Tarayıcıları

Güvenlik açıklarını veya boşlukları belirlemek, ağları ve bilgisayar sistemlerini taramak için güvenlik açığı tarayıcısı kullanılmaktadır. Bilgisayar korsanları, bir sistemdeki boşlukları tespit etmek için genellikle bu aracı kullanırlar. Böylece açıklar mümkün olan en kısa sürede düzeltilecektir. Siyah şapkalı bilgisayar korsanları, bir hedefin sistemindeki veya ağındaki zayıflıkları keşfetmek için güvenlik açığı tarayıcılarını kullanırlar.

4 BİR KİMLİK AVI SALDIRISINI TANIMA VE ÖNLEME

4.1 Kimlik avı nedir?

Çevrimiçi kimlik avı (phishing), bir e-posta iletisi veya web sitesi aracılığı ile kişisel ve finansal bilgileri elde etmek amacıyla, kullanıcıları kandırmak için kullanılan bir yöntemdir. En sık kullanılan kimlik avı dolandırıcılığıdır. Banka, kredi kartı şirketi veya bilinen bir online-çevrimiçi satıcı gibi bir kaynaktan gönderilmiş bir e-posta iletisiyle başlamaktadır. E-posta içerisinden, hesap numarası veya parola gibi kişisel bilgilerin istendiği sahte bir web sitesine yönlendirilmektedir. Bu bilgiler genellikle kimlik hırsızlığı amacıyla kullanılmaktadır.

Kimlik avı saldırıları, hem bireysel kullanıcılar hem de kuruluşlar için sorun teşkil etmektedir. Bir kişi veya kuruluştan elde edilen her türlü bilgi, saldırganın finansal avantajlar elde etmesine yol açmaktadır. Kimlik avı dolandırıcılığı siber ihlallerin en çok kullanıldığı yöntemler arasındadır.

4.2 Kimlik avı için kullanılan yöntemler

Bilgisayar korsanlarının kimlik avı saldırısını gerçekleştirmek için kullandığı bazı yöntemler şu şekilde sıralanmaktadır:

● Saldırgan, size gönderilen e-postalardaki bağlantıları değiştirmektedir. Bunu, URL'yi değiştirerek yapmakta, böylece kullanıcı kötü amaçlı bağlantı ile gerçek web sitesi arasındaki ayrımı yapamamaktadır. Örneğin, birçok web tabanlı uygulama "Şifremi Unuttum" özelliği sunmaktadır. Düğme tıkladığında, web sitesi şifre sıfırlamak için bir e-posta göndermektedir. Bilgisayar korsanı e-postayı yeniden yönlendirmeyi başarırsa, kullanıcı adının ve güvenlik sorusunun cevabının girildiği farklı bir bağlantı gönderecektir. Bilgisayar korsanı daha sonra hesaba erişmek için bu bilgileri kullanacaktır.

● Bazı bilgisayar korsanları, web sitesi sahteciliğini bir kimlik avı dolandırıcılığı aracı olarak da kullanmaktadır. Saldırgan orijinal görünen sahte bir web sitesi geliştirmek için JavaScript komutlarını kullanmaktadır. Bu, kullanıcıyı izlemeyi kolay hale getirmektedir.

● Saldırganlar gizli yönlendirme olarak bilinen bir tekniği kullanmaktadırlar. Bu süreçte, pop-up'lar atmak için (istem dışı açılan web sayfaları) gerçek web sitelerini kullanırlar. Bir kullanıcı, pop-up'ta açılan pencerede, kendisini saldırganın web sitesine yönlendiren bağlantılara tıklayarak veri ihlallerinin hedefi olmaktadır.

● Saldırganlar, virüslü EXE ekleri, PDF'ler ve Microsoft Office ekleri ile kullanıcının sistemine veya ağına kötü amaçlı yazılımları veya fidye yazılımlarını dağıtabilmektedirler.

● Saldırganlar, metin mesajları, telefon görüşmeleri, sosyal mecralar ve diğer medya yolları ile kimlik avı saldırıları gerçekleştirebilmektedirler.

4.3 Kimlik Avı Saldırılarıyla Mücadele Etmenin Yaygın Yolları

Sisteminizi ve ağınızı kimlik avı saldırılarından korumaya yönelik farklı yöntemler vardır. Kullanılan yaygın yöntemlerden bazıları şunlardır:

● Kötü Amaçlı Yazılım Tarayıcıları

● Otomatik Güncellemeler

● Çok Aşamalı Kimlik Doğrulama

● Sistem veya Veri Yedeklemeleri

Yukarıda bahsedilen yöntemlere ek olarak, sisteminizi ve ağınızı kimlik avı saldırılarından korumak için kullanabileceğiniz başka teknikler de vardır.

4.3.1 Aldatıcı Kimlik Avı

Aldatıcı kimlik avı, en yaygın kimlik avı saldırısı türlerindendir. Saldırgan, kullanıcının kişisel bilgilerini veya giriş bilgilerini vermesi için gerçek bir e-posta göndereni veya kuruluşu taklit etmektedir. Bu, e-postalar kullanılarak yapılmaktadır. E-posta içeriği, kullanıcının paniğe kapılmasına neden olmakta ve saldırganın yapmak istediği şeyi tam olarak yapmasına neden olan bir aciliyet duygusu yaratmaktadır.

Örneğin, saldırgan bir veya daha fazla kullanıcıya e-posta gövdesindeki bağlantıyı kullanarak ödeme yapmazlarsa kredilerinin devre dışı bırakılacağını bildiren bir e-posta göndermektedir. Kullanıcı bağlantıyı tıkladığında, bankanın veya ödeme ağ geçidinin bir kopyası, kullanıcıyı saldırganın web sitesine yönlendirmektedir. Kullanıcı daha sonra son kullanma tarihi ve güvenlik kodu dâhil olmak üzere kredi kartı bilgilerini girer. Saldırgan artık, kullanıcının kredi kartında hileli işlemler yapmak için gerekli tüm bilgilere sahip olmuştur.

Aldatıcı bir kimlik avı saldırısının başarısı, kimlik avı e-postasının gerçek kuruluşun e-postasına ne kadar benzediğine bağlıdır. Kullanıcıların, bağlantıyı tıklamadan veya herhangi bir bağlantıyı indirmeden önce kendilerini korumak için hem e-posta

adresinin hem de e-posta gövdesindeki bağlantıların URL'lerinden geçmesi gerekir. Aldatıcı bir kimlik avı e-postasının sahteliği yazım ve dilbilgisi hataları ile genel selamlamalardan anlaşılmaktadır.

4.3.2 Yemleme kancası (Spear phishing)

Teknolojilerin sağladığı imkânları kullanmak suretiyle, hedef alınan kişilerin aldatılarak, ikna edilerek kişisel veya gizli verilerinin ele geçirilmesidir. Bu söz konusu verilerin kötü niyetle kullanılması olarak da tanımlanmaktadır. Bunun ilk örneklerinden birisi 1960'larda telefon sistemlerine yetkisiz olarak giren kişilerin kendilerini ''Phone Phreaks'' olarak isimlendirmesiyle görülmüştür. Burada ucube, garabet, çılgın gibi anlamlar taşıyan ''Freak'' kelimesi dönüştürülüp ''Phreak'' şeklinde yazılarak bu terim türetilmiş ve yaygın olarak kullanılmıştır. ''Phishing'' kelimesinin de bu şekilde türetilmiş bir terim olduğu düşünülmektedir.

4.3.3 Balina Saldırısı (Whale Attack)

Bir yapıdaki üst düzey yöneticiler dahil herkese saldırmak için kullanılmaktadır. Saldırgan, bilgileri ve oturum açma kimlik bilgilerini çalmak için patronları ve üst düzey yöneticileri hedef almaktadır. Başarılı bir balina avı saldırısı, CEO dolandırıcılığına yol açmaktadır. Adından da anlaşılacağı gibi, CEO dolandırıcılığı, saldırganın banka bilgilerini aldıktan sonra büyük finansal işlemleri onaylamak için CEO'nun e-postasını kullandığı yerdir. Balina avının bir başka uygulaması da, saldırganların yöneticinin e-posta hesabını kullanarak, diğer çalışanların kişisel bilgilerini talep etmesidir. Çalışanların bilgilerini kullanarak, sahte vergi beyannamesi düzenleyerek finansal anlamda veri sahteciliği yapılmaktadır. Ayrıca saldırgan bu bilgileri çevrimiçi olarak satmaktadır.

Kuruluşlardaki üst düzey yönetim, bilgi güvenliği konusunda eğitimli olduğundan çoğu saldırganın balina avı saldırılarından kurtulmaktadır. Üst düzey yönetim de dâhil olmak üzere tüm çalışanlar için güvenlik bilinci eğitimi zorunlu hale getirilerek balina avcılığından kaçınılabilecektir. İşletmelerin ayrıca finansal işlemlerini yalnızca e-posta yoluyla gerçekleştirmemeleri için iki faktörlü kimlik doğrulama veya çok faktörlü kimlik doğrulama süreçleri uygulanması daha doğru olacaktır.

4.3.4 Vishing – Smishing

Vishing yöntemi, kurbanı ses ile aldatma yöntemidir. Bu nedenle ‘’Phishing’’ kelimesindeki “p” harfinin yerine ‘’Voice’’ kelimesinin ilk harfi kullanılarak “Ses Aldatmacası” anlamında kullanılmaktadır. Vishing dolandırıcılık metodu, müşterilerin kişisel bilgilerini elde etmeye yönelik gönderilen e-postalar olarak nitelendirilmektedir. Bu e-postaların içeriklerinde verilen çeşitli telefon numaralarına yönlendirmeler yapılmaktadır. Bu sahte telefon numaraları kurban tarafından arandığında, dolandırıcının daha önceden hazırladığı sesli yanıt sistemlerine yönlendirilmektedir. Bunlar banka sesli yanıt sistemini ve çağrı merkezini taklit eden bir sistem olarak tanımlanmaktadır. Dolandırıcılar bu yöntem sayesinde kurbana ait kişisel bilgileri ele geçirmektedir. Vishing saldırıları sadece e-posta yoluyla değil, cep telefonlarına gönderilen bir mesaj ile de yapılabilmektedir. Bunada ‘’Smishing’’ denir. ‘’Ücretsiz sms gönderin, X TL puan kazanmak için kaydolun.’’ tarzında faaliyet gösteren dolandırıcılık yöntemidir. Bir site gibi kayıt sırasında, kullanıcı bilgileriyle beraber cep telefonu numaranızı elde edip, daha sonra kiralanan bir hat üzerinden toplu sms gönderilerek yapılabilmektedir. Cep telefonlarına ulaşan mesajın içeriği, gönderilen e-posta içeriğine benzer olmakta ve yine benzer senaryolarla bilgilerinizi ele geçirmeyi hedeflemektedir. Pandemi döneminde bu saldırı yöntemi artış göstermiştir. Aşı randevusu adı altında mesajlar yollanarak, dolandırıcılar kişisel bilgilerin girildiği yerlere yönlenerek insanların bilgilerini almaya çalışmışlardır. Vishing'i önlemenin en basit yolu, bilinmeyen numaralardan gelen aramaları asla yanıtlamamak, arayan kimlik bilgisi için bir uygulama kullanmak ve kişisel bilgileri telefon üzerinden kimseye ifşa etmemektir. Smishing saldırısından kaçınmanın en basit yolu ise size mesaj gönderen numaraya bakmak ve ardından bununla ilgili bir şeyler yapmaya karar vermektir. Alternatif olarak, mesajda belirtilen şirketi aramak ve gerçekten böyle bir mesaj gönderip göndermediklerini kontrol etmek bir çözüm olacaktır.

4.3.5 Pharming

‘’Pharming’’ web sitesi trafiğinin manipüle edildiği ve gizli bilgilerin çalındığı kimlik avına benzer bir siber suç türüdür. Site trafiği yönlendirme, internet taramasının çalıştığı zeminden faydalanmaktadır. Bağlantı kurulabilmesi için ‘’www.google.com’’ gibi bir internet adresini oluşturan harflerin sırasının DNS sunucusu tarafından bir IP adresine dönüştürülmesi gerekmektedir. Bu tehdit için iki saldırı yöntemi vardır: Birincisi, korsan bir kullanıcının bilgisayarına trafiği asıl hedeften başka yere yönlendirmektir. Sahte bir web sitesine göndermek için, bilgisayarın ana bilgisayardaki dosyalarını değiştiren bir virüs veya truva atı yüklenmektedir. İkincisi ise, korsan bir DNS sunucusunu değiştirerek, birden çok kullanıcının farkında olmadan bu sahte siteyi ziyaret etmesine neden olmaktadır. Sahte web sitesi, kullanıcının bilgisayarına virüs veya truva atı yüklemek amacıyla kullanılmaktadır. Kimlik hırsızlığında kullanılmak üzere kişisel ve finansal bilgileri toplama girişimi de olabilmektedir. ‘’Site Trafiği Yönlendirme,’’ özellikle endişe verici bir siber suç biçimidir. Çünkü DNS sunucusunun değiştirilrmesi durumunda bundan etkilenen kullanıcı hiç kötü amaçlı yazılım bulunmayan bir bilgisayara sahip olsa bile kurban haline gelebilmektedir. Web sitesi adresini manuel olarak girme veya daima güvenilen yer imlerinin kullanılması gibi önlemler almak yeterli olmamaktadır.

Bu tür dolandırıcılıktan korunma; şüpheli web sitelerinden kaçınma ve şüpheli e-posta iletilerindeki bağlantılara asla tıklamamaktır. Bilgisayar kullanma uygulamalarıyla birlikte kullanılmak üzere, güvenilir bir kötü amaçlı yazılım ve virüs karşıtı çözümün yüklenmesiyle korunulabilmektedir. Bu adımlar çoğu kötü amaçlı yazılımın bilgisayara erişmesini ve ana bilgisayar dosyalarını değiştirmesini önlemektedir.

4.4 Bir Kimlik Avı E-postasını Tanımlama

Bir kimlik avı e-postasının neye benzediğini, nasıl tanımlanacağını ve bu tür e-postalarla kandırılmamak için hangi önlemlerin alınması gerektiğinin bilinmesi gerekmektedir.

4.4.1 E-posta Sahtekârlığı

Saldırganın, bir e-postanın başlıklarını manipüle ederek e-postanın kaynağının, saldırganın sistemi gibi meşru olmayan bir kaynaktan geliyor gibi gösterilmesidir. Bu e-postanın gerçek görünmesini sağlayan kimlik avı çatısı altında bir metodolojidir. Saldırganlar, gönderenin e-posta adresini daha önce gördükleri bir adrese benzediği için, kullanıcıların e-postaya güvendiklerinin farkındadır. E-posta sahtekârlığının amacı, kullanıcıyı aldıkları e-postanın önemli olduğuna ve gönderenin gerçekten bilgi talep ettiğine inandırmaktır.

4.4.2 Sahte Bir E-postayı Tanımlama

Sahte bir e-postayı belirlemenin iki yolu vardır:

Konu satırı verilen örneklerden herhangi birine benziyorsa, e-posta gerçek değildir:

● abc@example.com e-posta hesabınız saldırıya uğradı.

● Acil: E-posta hesabınızın şifresini hemen değiştirin.

● Banka hesabınız ele geçirildi.

● Güvenlik Uyarısı: E-posta hesaplarınızı kaydedin.

Size yollanan E-posta içeriği aşağıdaki bilgileri isterse, sahte bir e-postadır:

● Kişisel bilgileriniz veya banka hesabı ayrıntılarınız,

● Belirli bir hesaba para göndermenizin istenmesi,

● Parola değişikliği istememiş olmanıza rağmen parola sıfırlama bağlantısı gelmesi,

● Ayrıntıları doğrulamak için diğer bilinmeyen bağlantılara yönlendirilmek.

‘’E-postanın gerçekten de e-posta başlıklarından gelen sahte veya spam bir e-posta olduğunu nasıl doğrularsınız?’’ diye bir soru gelmektedir. E-posta kaynağında aşağıdaki parametrelerden birine bakarak e-postanın gerçekliği doğrulanmaktadır.

4.4.3 Alınan-SPF

SPF (Sender Policy Framework) Domain DNS kayıtlarında, o domain adının hangi IP adreslerinden e-posta gönderdiğini belirten TXT kayıtlarına verilen isimdir. E-posta gönderimlerinde gönderici için "Kimlik İbrazı" da denir. Özellikle Hotmail, Yahoo, Gmail gibi e-posta servislerinin kontrol ettiği SPF kayıt doğrulaması ile ISS'ler, aldıkları e-posta mesajının, gönderim yapılan sunucu ile gönderici e-posta adresinin gerçek gönderici olduğunu teyit etmek ister. Bu kaydı oluşturmanın amacı, e-postaların gerçekten doğru yerden geldiğini teyit etmek ve spoof sahte e-postaları engelleyerek, phishing saldırılarını engellemektir.

4.4.4 X-CMAE Puanı - 100

Bu, e-postanın spam puanıdır. Alıcı e-posta sunucusu, e-postaya hangi spam puanını atadığına bağlı olarak belirli spam kontrollerine sahiptir. En yüksek değer 100'dür. Bir e-postanın başlığı bu şekilde görünmektedir. Üstbilgiye, e-posta sağlayıcısının arayüzünde, bir e-postanın orijinal kaynağını ''gmail.com'' gibi görüntüleyerek erişilebilmektedir.

Bir kullanıcı böyle bir e-posta aldığında akıllara bazı sorular gelmektedir. Böyle bir e-posta alınırsa hesap tehlikeye girer mi? Hayır, e-posta hesabı hiçbir şekilde tehlikeye girmez. Alınan e-posta ya spam ya da sahte bir e-postadır. Sunucu neden bu tür e-postaları SPAM olarak sınıflandırmıyor? Çoğu sunucu, bu e-postaları SPAM olarak sınıflandıran sıkı e-posta kontrollerine sahiptir. Bu e-postalar otomatik olarak kullanıcının e-postasının spam klasörüne taşınır, ancak bu kontrollerin bir e-postayı atlayabileceği unutulmamalıdır. Sahte bir e-posta almaktan tamamen kaçınabilir mi? Hayır, her durumda, spam yapan kişi farklı bir konu ve farklı bir gövde kullanabilir. Bu nedenle genel bir filtre oluşturmak işe yaramayacaktır. Bu filtre yasal e-postaları engelleyebilmektedir.

4.4.5 Referans E-postası: (Kullanılan Şablon)

"Merhaba yabancı! Size bu mesajı hesabınızdan gönderdiğim için cihazınızı hackledim." Şifrenizi zaten değiştirdiyseniz, kötü amaçlı yazılımım her seferinde onu yakalar. Beni tanımıyor olabilirsiniz ve büyük olasılıkla bu e-postayı neden aldığınızı merak ediyorsunuz, değil mi?

Aslında, bazı web sitelerinin yetişkinleri (pornografi) üzerine kötü amaçlı bir program yayınladım ve bu web sitelerini eğlenmek için ziyaret ettiğinizi biliyorsunuz (ne demek istediğimi biliyorsunuz). Siz video klipleri izlerken, benim Trojan'ım hem ekranınıza hem de bir web kamerasına erişmeme izin veren bir keylogger ile bir RDP (uzak masaüstü) olarak çalışmaya başladı.

Bundan hemen sonra, programım tüm bağlantılarınızı messenger, sosyal ağlar ve ayrıca e-posta yoluyla topladı. Ben ne yaptım Çift ekranlı bir video yaptım. İlk bölüm izlediğiniz videoyu gösterir (iyi bir zevkiniz var, evet ama diğer normal insanlar ve benim için garip) ve ikinci bölüm web kameranızın kaydını gösterir.

Saldırgan bu e-postayı, gönderdiği kişinin kendi e-posta adresini taklit etmektedir. Kullanıcının e-posta hesabına erişimi olduğuna inandırarak e-postayı göndermektedir. İçeriğe bakarsanız, saldırgan masum bir kullanıcıyı, kullanıcının bilgisayarına erişemediği zaman bile, erişebileceğini söyleyerek ikna etmeye çalışmaktadır. Kullanıcı dikkatli olmazsa saldırgana inanarak, isteklerini yerine getirecektir. Ancak, e-postanın başlıklarını incelemek, kullanıcının bu saldırganın gerçekten e-postalarına erişimi olup olmadığını veya blöf yapıp yapmadığını anlamasına yardımcı olacaktır.

Her kimlik avı girişimini tanıyabileceğinizin garantisi yoktur. Saldırganlar ayrıca araştırma yaparak, kullanıcı davranışları hakkında daha fazla bilgi edinmektedirler. Bu bilgileri, saldırılarını iyileştirmek için kullanmaktadırlar. Bunu unutmayarak, kullanıcılar, korsanların bugün kullandığı yeni kimlik avı teknikleri hakkında daha fazla bilgi edinmeli ve bu konuda kendilerini eğitmelidirler.

5 KÖTÜ AMAÇLI YAZILIM NASIL BELİRLENİR VE KALDIRILIR

Kötü amaçlı yazılım, farklı kötü amaçlı yazılımlar için (casus yazılımı, fidye yazılımı ve virüsler gibi) kullanılan genel bir terimdir. Kötü amaçlı yazılım, saldırganlar tarafından bir sisteme ve ilgili verilere saldırmak için geliştirilen bir koddur. Kötü amaçlı yazılımları dağıtmak için kullanılan araç genellikle bir e-posta olmaktadır. E-

posta, tıklandığında veya indirildiğinde kötü amaçlı yazılım kodunun yürütülmesine neden olan bağlantılar veya ekler çalıştırılmış olmaktadır.

Kötü amaçlı yazılım, bireysel kullanıcıları ve kuruluşları tehdit eden ‘’Creeper Virüsü’’ 1970'lerin sonunda ortaya çıkmıştır. O zamandan beri dünya, hepsi aynı amaca sahip milyonlarca kötü amaçlı yazılım görmüştür. Bunların amacı hep aynıydı. Hizmetlerin kesintiye uğratılması ve yok edilmesiydi. Kötü amaçlı yazılım, çeşitli şekillerde hedef sistemlere dağıtılan yükleri içermektedir. Bir saldırganın güdüleri para istemekten bilgi çalmaya kadar uzanmaktadır. Saldırı teknikleriyle daha da akıllı hale gelmeye başlamaktadırlar.

5.1 Kötü Amaçlı Yazılım Türleri

Birinci bölümdeki siber güvenlik terminolojisi bölümünde bu terimlerin bazılarından daha önce kısaca bahsetmiştik. Bunlardan şimdi biraz daha ayrıntılı bahsedelim.

5.1.1 Virüsler

Bilgisayar virüsleri biyolojik virüsler gibidir. Çalışmanızı engeller ve iyileşmek için birçok yola başvururuz. Bu nedenle “virüs” olarak adlandırılırlar. Biyolojik virüslerin bir insandan diğerine geçmesi gibi bilgisayar virüsleri de bir bilgisayardan diğerine geçmektedirler. Bilgisayar virüsleri durmak bilmeden çoğalmak amacıyla geliştirilmiştir. Kendilerini başka bir programa, belgeye veya önyükleme kısmına kopyalayarak çoğaltan kötü amaçlı yazılımlardır. Bu virüsler, bilgisayarın çalışma şeklini, işletim sisteminin bütünlüğünü ve gizliliğini tehdit etmektedir. Bilgisayar virüslerinin, kendilerini bir kullanıcının bilgisi veya izni olmadan çoğaltmaları gerekmektedir. Bu anlamda bilgisayar virüsleri birer bağımsız program değildirler. Bu virüsler Fidye Yazılımları, Truva Atı (Trojan Horse Virus), Solucan Virüsü gibi birçok kötü amaçlı yazılımı bünyesinde bulundurmaktadır. Bilgisayar virüsü diğer kötü amaçlı yazılım türleri gibi bilgisayarınıza zarar vermek ve ele geçirmek amacıyla saldırganlar tarafından oluşturulmuştur. Bilgisayar virüslerinden korunma konusunda ne kadar dikkatli ve bilinçli olursanız olun nereden geldiğini tahmin edemeyeceğiniz yerlerden bilgisayarınıza virüs bulaşabilir. İnternet kullanımı henüz yaygın değilken virüsler, genellikle virüslü disklerden bilgisayarınıza ve oradan da başka bilgisayarlara yayılıyordu. Modern zamanda ise bunlar, sizinle paylaşılan müzikler, fotoğraflar, e-

postalar, indirilen oyunlar, programlar, uygulamalar ya da virüs bulaşmış bir web sitesi ziyaretinden kaynaklı olmaktadır. Virüsün bulaşma işlemi genellikle kullanıcının kendi isteğiyle ya da farkında olmadan virüslü bir program yürütmesiyle gerçekleşmektedir. Bilgisayar virüsü içeren bir program çalıştırıldıktan sonra, bu virüs belleğe taşınmaktadır. İşte tam bu noktada virüs, bilgisayardaki diğer uygulamalara hızla bulaşmakta ve kötü amaçlı kodunu yayabildiği kadar yaymaktadır. Bilgisayarların disket önyükleme kısımlarına bulaşan önyükleme virüsleri bu aşamada özellikle zararlı bir teknik kullanmaktadırlar. Bu kodları ön yüklemeye yerleştirerek bilgisayarın normal bir şekilde çalışmasını bile imkânsız hale getirmektedirler. Bazen bir e-posta eki açarak veya virüslü bir reklama tıklayarak yayılabilen bilgisayar virüsleri, ana makineye ulaştıktan sonra kendini belleğe yüklemekte ve çalıştırılan her programa bulaşmaktadır. Bu virüsler sistem yazılımlarına ulaşıp verileri kopyalayabilir, silebilir veya şifreleyebilirler. Bilgisayar virüsleri bulaştıkları programları ya anında ya da zaman içinde işlemez duruma getirmektedir. Bilgisayar virüslerinin bazıları, programların tamamen silinmesine, dosyalara erişilmemesine ve sistemin çökmesine neden olmaktadır. Eğer bilgisayarınızda sebebini bilmediğiniz veri kaybı, performans düşüşü, sık sık bilgisayar çökme problemi yaşıyorsanız bilgisayarınıza virüs bulaşmış demektir. Elbette bilgisayarınıza virüs bulaşmaması için birçok yöntem vardır. Anti-virüs programları ve casus yazılımları bu konuda en büyük etkenlerdendir. Ayrıca kullanılan işletim sisteminin ve tarayıcıların güvenlik ayarlarını sürekli güncel tutarak, yalnızca güvenilir sitelerden yazılım indirerek veri güvenliği sağlanabilir. Ayrıca tanımadığınız adreslerden gelen e-postalar açılmamalı ve spam mailleri silinmelidir. Çünkü gönderilen basit bir e-postada bile zararlı yazılımlar olabilir. Bilinçsizce bu işlemler yapıldığında virüslü uygulama yürütülmekte ve virüs CPU belleğinize kadar yayılabilmektedir. Böylece bilgisayar virüsü diğer uygulamalarınıza da bulaşarak kötü amaçlı yazılım kodu ulaşabildiği her yere yayılmaktadır.

● Bu virüsler banka kimlik bilgilerinizi tarayabilir,

● Şifrelerinizi çalmak için tuş hareketlerinizi izleyip kaydedebilir,

●Verilerinizi şifreleyip geri alabilmeniz için sizden fidye/bitcoin ödemesi isteyebilirler.

Bilgisayarda ücretsiz anti-virüs programları olsa da korunmak için güvenilir ve güncel bir korumaya ihtiyaç duyulmaktadır. Anti-virüs programları virüslere karşı koruma sağlayan, kurtarma ve temizleme işlerini yapan koruyucu programlardır. Bu programlar bilgisayarınızdaki virüsleri tespit edip karantina ve silme işlemlerini gerçekleştirmektedir.

5.1.2 Solucanlar-Wormlar

Solucanların bilinen tarihi virüslerden öncedir. Bilgisayarların geliştirilmesinden bu yana var olmuşlardır. 1990'larda e-postanın kullanıma girmesiyle popüler hale gelmişlerdir. Birçok kullanıcı e-posta ekleri ile birlikte gelen solucanlarla ciddi sorunlar yaşamıştır. Bir çalışan, solucan içeren bir e-postayı açtığında tüm kuruluş kısa sürede etkilenmektedir. Solucanlar bulaştıkları sistemlerde kendilerini çoğaltarak sistemde yayılmaya başlarlar. Teknik anlamda katlanarak çoğaldıkları (kendini kopyalama) için çok kısa bir zaman içinde çok büyük rakamsal değerlere ulaşırlar. Wormlar temel anlamda insanlara benzerler kendi soylarını devam ettirme çabası içinde kendi kopyalarını (klon) ulaştığı her ortama yaymaya çalışırlar. Böylece hayatta kalma süreleri uzayarak verdiği zararlar katlanarak artmaktadır. Gerçek hayatta solucan gibi canlılar ortadan ikiye bölündüğünde iki farklı yeni canlı oluşmaktadır. Bu zararlı ise bölünmek yerine kendini çoğaltarak sayısını arttırır. Wormlar kodlandığı dile göre çeşitlilik gösterse de özünde normal dosya kopyalama şeklinde olduğu gibi çoğalmaktadırlar. Wormlar çalıştırılan makinede zararlı kodların bir kopyasını oluşturup daha sonra farklı bir konumda tekrar bir araya getirirler. Kendisinin aynısı (klon) olan bir worm meydana getirirler. Kopyalama işlemi bilinen dillerde olan sistem kütüphanelerini işleyerek tek satırda gerçekleştirilebilir. Worm virüsünün önemli noktalarından biri olan insan faktörünü kullanması onu olduğundan daha tehlikeli hale getirmektedir. Bir klasör altına klasör ile aynı isimde bir kopyasını meydana getirerek aktif olması ile, wormun tekrar tetiklenmesi için insanların zafiyetini kullanır. Worm bununun yanında kendisini disk, çıkarılabilir medya, harici bellek, disk gibi ortamlara "Özel Dosyalar" ismiyle çoğaltmaktadır. Bu durumdaki amaç meraklı kişilerden faydalanılarak kendisinin sisteme bulaştırılmasını sağlamaktır. Wormların diğer bir özelliği de "autorun. inf" adında otomatik başlatma için kullanılan bir dosyayı harici belleğe yazarak, bellek sisteme takıldığında otomatik tetiklenmeyi sağlar. (Eski sistemler için geçerli). E-Posta içindeki ekleri ile de yayılabilen bu wormlar,

kullanıcıların kişiler listesindeki kişilere otomatik oluşturulan bir e-mail atarak ekine kendisinin bir kopyasını yerleştirirdi. Her yönüyle kendi kopyalarını olası bütün koşullarda çoğaltmayı hedefleyen bu zararlı yazılımların spesifik olarak birçok özelliği daha bulunmaktadır. Bu virüs çeşitleri genel olarak ilk başlarda kendilerini çoğaltmayı amaçladıklarından bilgisayara zarar verdikleri düşünülmeyebilir. Zamanla kullanıcının birçok bileşenine erişimini engelleyerek kendisinin sisteme olabildiğince fazla zarar vermesini sağlıyor. Bunlara örnek olarak: o Görev yöneticisini devre dışı bırakma o Regeditin (kayıt defteri) kapatılması o ‘’Gizli dosyaları göster’’ seçeneğini aktif hale getirildiği halde tekrar pasif hale getirme o Masaüstü dosyalarına erişimi engelleme o Başlat menüsündeki araçların bağlantılarını değiştirme o usb belleklerde kendisinin gizli bir kopyasını oluşturma o Bilgisayardaki CPU (Merkezi İşlem Birimi) yük artırma o Bilgisayardaki Ram’e (Rastgele Erişim Belleği) yük bindirme o Bilgisayarda ikincil diskin (HDD, SSD) devamlı kullanılmasına neden olma (kopyalama ve kontrol işlemlerinden dolayı) o Bilgisayarın Hafızasında yer işgal etme (her oluşturulan kopya depolama biriminde bir yer tayin eder.) Daha birçok etkisi olmasının yanında bunlar genel anlamda kabul görenleridir. Solucanlar (worm) diğer virüslerle kıyasla daha kolay dezenfekte edilebilen virüslerdir. Bilgisayarlardaki güncel olan antivirüsler neredeyse tüm worm virüslerini tanır ve temizler. Yalnız önem verilmesi gereken kısım, disklerin dizinlerle birlikte tarama işleme tabi tutulmasıdır. Bunun nedeni virüsün yayılması sonucu olası her dizin altına bir kopyasının oluşturmuş olma ihtimalidir. Diğer virüslere kıyasla bilgisayardan temizlenme süreci oldukça uzun sürmektedir. Bunun nedeni antivirüsün bütün alt dizinleri ayrı ayrı tarayarak virüsün varlığını kontrol ediyor olmasıdır. Manuel bir şekilde temizlemek olası bir ihtimal olsa da en pratik yol bu tür virüslere karşı üretilmiş antivirüs ve antimalware yazılımlarıdır. Genellikle temizleme işlemi ardından bazı bölümler (regedit, task manager) kendiliğinden düzeltilemez. Bunun için kolaylıkla bulunacak birçok düzeltme aracı vardır. Virüsün temel olarak yaptığı regedit (kayıt defteri) değerlerini değiştirerek ilgili görev yöneticisine erişimi kısıtlamaktır. Burada diğer üçüncü parti araçlarla bu kayıtlar düzeltilebilmekle birlikte script ile sorunlar düzeltilmektedir. Bazı worm türleri antivirüslerini de engellediğinden bilgisayarı “güvenli” modda başlatmak sorunu çözmek için en iyi çözümlerden biridir. Genelde insanlar arasında bilgisayara format atmak da olası çözümler arasında yer alsa da

format (sistem sıfırlama) işleminden sonrası alınan yedekler için detaylı bir virüs taraması yapmak gerekmektedir.

5.1.3 Truva Atları

Saldırganlar, yeni saldırılar uygulamak için bir silah olarak solucanlardan Truva atlarına geçti. Truva atları, gerçek programlar veya dosyalar gibi görünseler de içlerinde kötü amaçlı kodlar bulunmaktadır. Truva atları dijital dünyada virüslerden önce mevcuttu ve bugün siber suçlar arasında en popüler kötü amaçlı yazılımlardandır. Virüsler gibi, Truva atları da yürütülmesi için kullanıcı etkileşimine ihtiyaç duymaktadır. Truva atı, hedef sisteme ulaşmak için bir araç olarak e-postaları veya kötü amaçlı web sitelerini kullanmaktadır. En yaygın ve popüler Truva atı türü sahte bir virüsten koruma yazılımıdır. Belirli web sitelerini ziyaret ederken bilgisayarınıza virüs bulaştığını söyleyen bannerler vardır. Sizden virüsü temizlemek için yazılımın indirilmesini isteyecektir. Bunun doğru olduğuna inanarak, Truva atı indirilip yüklenebilir. Truva atı daha sonra sisteminizin kontrolünü ele geçirmektedir. Kendinizi bir Truva atına karşı savunmanız iki nedenden dolayı zordur:

● Truva atlarını kodlamak kolaydır ve siber suçlu grupları bugün Truva atı oluşturma kitleri bile geliştirmiştir.

● Truva atları, kullanıcıları kandırarak bir sisteme yerleştirilir ve bu nedenle bir güvenlik duvarı gibi geleneksel savunmalardan rahatlıkla kaçarlar.

Kelimenin tam anlamıyla her ay geliştirilen milyarlarca Truva atı bulunmaktadır. Virüsten korunmak için geliştiriciler, Truva atlarına karşı koymak için ellerinden geleni yapmakta, ancak imzaları izlenemeyecek kadar fazla olduğundan bu konuda zorlanmaktadırlar.

5.1.4 Hibrit Kötü Amaçlı Yazılım

Hibrit kötü amaçlı yazılım; diğer kötü amaçlı yazılımların, Truva atlarının ve hatta virüslerin karma bir kombinasyonudur. Kötü amaçlı yazılım başlangıçta bir Truva atı gibi görünebilir. Ancak yürütüldüğünde, solucanlar tarafından ağdaki tüm kullanıcılara saldırmaktadır. Günümüzde kötü amaçlı yazılım programları, gizli programlar veya rootkit'ler olarak kabul edilmektedir. Bu da günümüzde kötü amaçlı

yazılımın temel amacının, bilgisayarın işletim sisteminin kontrolünü ele geçirmek ve kötü amaçlı yazılım önleme programlarının bile algılayamayacağı şekilde onu manipüle etmek olduğu anlamına gelmektedir. Bu tür kötü amaçlı yazılımlardan kurtulmanın tek yolu, sistemin kontrolüne sahip olan bellek bileşeninin bağlantısının kesilmesidir. Botlar kendilerini ayrı bilgisayar sistemlerine yerleştirir ve ardından bot ağı için komuta ve kontrol sunucuları olan bot yöneticilerinden talimat beklerler. Botnet olarak bilinen bot ağları, tek bir botmaster tarafından kontrol edilmektedir. İnternet üzerinden binlerce sunucudan oluşan bir ağla birkaç yüz bilgisayarı istila edebilirler. Bot yöneticileri genellikle bu botnet'leri, onları özel ihtiyaçları için kullanan diğer suçlulara kiralamaktadırlar.

5.1.5 Fidye Yazılımı

Fidye yazılımı, her geçen gün gelişen ve daha da yaygınlaşan bir zararlı yazılım türüdür. Temelde iki türü vardır: Şifreleyiciler ve kilitleyiciler. Bilgisayarınıza şifreleyici bulaştığı zaman, bilgisayarınızda bulunan her türlü veriyi (dosyalar, fotoğraflar, oyunların save dosyaları, veri tabanları vs.) şifrelemektedir. Dosyalar bir defa şifrelendiğinde dosyaları açamazsınız ve dosya içerisinde bulunan verilere ulaşamazsınız. Bu saldırıları düzenleyen suçlular, dosyalarınızı açabilecek özel anahtar karşılığında fidye talep etmektedirler. Talep edilen ortalama fidye miktarı 3000 TL civarıdır. Diğer türe kilitleyici denilmesinin sebebi ise, bu zararlı yazılımların bütün cihazı kilitlemesidir. Yani sadece dosyalarınız değil, bütün sistem erişilmez olmaktadır. Kilitleyicilerin istedikleri fidye miktarı şifreleyicilerinki kadar yüksek olmamaktadır. Tüm Windows, Mac OS X, Linux ve Android cihazları tehdit etmektedirler. Kısacası tüm masaüstü ve mobil cihazlar tehdit altındadır. Ancak fidye yazılımları ağırlık olarak Windows ve Android cihazları hedef almaktadır. Aynı zamanda cihazınıza bulaşması da çok kolaydır. Çok yaygın olarak, fidye yazılımları bilgisayarda açılan şüpheli eklerden, tıklanan şüpheli linklerden ve uygulama indirilen üçüncü parti mecralardan bulaşmaktadır. Ayrıca fidye yazılımları yasal internet sitelerine de bulaşabilmektedir. Güncel olarak, siber suçlular fidye yazılımlarını kullanıcılara bulaştırmak için reklam ağlarını kullanırlar. Kullanıcılara önemli bir şey indirtip açtığını düşündürmek çok zor olmamaktadır. Bankadan gelmiş bir mail ya da önemli bir program yüklemesi bunlardan bazılarıdır. Dosya açıldığında ya da program kurulduğunda, kullanıcı kendi bilgisayarına fidye yazılımı kurmuş olmaktadır. Fidye

yazılımlarının temel sorunu şu ki zararlı yazılımı silmeniz ile problem çözülmüyor. İyi bir antivirüs programı ve özellikle belli uygulamalar, genellikle fidye yazılımlarına karşı çok etkili çözüm sunmaktadır. Eğer zararlı yazılım dosyalarınızı şifrelerse, verilerinize erişebilmek için şifreyi bilmeniz gerekmektedir. Bu şifreye de ancak para ödeyerek erişebilirsiniz.

5.1.5.1 Enfekte Olunursa Ne Yapılmalıdır?

Fidye yazılımı kurbanı olunursa uyulması gereken temel kural, asla fidye ödememektir. ‘’Emniyet Siber Suçlar Birimi’’ bile fidye ödememenizi tavsiye etmektedir. Fidye ödenirse, saldırganların yapmak istediği şeyler yapılmış olunmaktadır. Bu nedenle, onları gelecekte fidye yazılımı saldırıları planlamaya teşvik edersiniz. Ücretsiz dosya şifre çözme yazılımlarını kullanarak şifrelenmiş dosyalardan bazılarını geri alma olasılığı ne yazık ki düşüktür. Ancak, bu araçların tersine çevirebileceği veya önleyebileceği bazı fidye yazılımı saldırıları vardır. Ayrıca, bir şifre çözücü varsa, sisteminizde zaten mevcut olan fidye yazılımlarından korumaya yardımcı olduğundan emin olunmalıdır. Dosyalarınız daha fazla şifreleneceğinden herhangi bir şifre çözme yazılımının bilgisizce çalıştırılmaması gerekmektedir. Fidye yazılımlarını temizlemenin diğer bilinen yöntemleri ise, sisteminizi taratmak ve bulaşımı ortadan kaldırmak için fidye yazılımı önleme ürünlerini kullanmaktır. Bu çözümler dosyalarınızı geri almanıza yardımcı olmayacaktır. Ancak sisteminizin temizlenmesine yardımcı olacaktır. Ekran kilidi durumunda, sistemi önce, sağlıklı bir geri yükleme noktasına geri yüklemeyi denemeli veya ön yüklenebilir bir USB sürücüden veya DVD'den bir tarama yapması denenmelidir.

Devam eden bir fidye yazılımı saldırısını bertaraf etmek istiyorsanız, her zaman tetikte olunmalıdır. Sisteminizde sebepsiz yere yavaşlama olduğunu fark ederseniz, en iyisi sistemi yeniden başlatmak ve internet bağlantısını kesmek olacaktır. Bu, sistemi başlattığınızda kötü amaçlı yazılımın etkin olmamasını sağlayacaktır. Ayrıca komuta edilen sunucudan veya saldırgandan talimat alamayacak veya gönderemeyecektir. Saldırganın, etkinliği tamamlamadığı için sistemdeki tüm dosyaları şifreleyemeyeceği ve dolayısıyla para talep edemeyeceği anlamına gelmektedir. Bu noktada, kötü amaçlı yazılımdan koruma çözümü yüklenmeli ve sistemde tam bir tarama gerçekleştirilmelidir.

5.1.5.2 Fidye Yazılımından Nasıl Korunuruz?

Bir fidye yazılımı bulaşmasıyla mücadele etmenin birkaç yöntemi bulunmaktadır. Ancak bunların işe yaradığına dair bir kanıt bulunmamaktadır. Bunların çoğu üst düzey teknik uzmanlık gerektirir ve orta düzeyde bir kullanıcı bu tür araçları kullanamaz. Bu nedenle, aşağıdaki çözüm yolları izlenmelidir.

İlk adım olarak, gerçek zamanlı koruma sağlayan ücretli yazılımlar satın alınmalıdır. Bu çözüm aynı zamanda gelişmiş fidye yazılımlarından gelen saldırıları da algılayacaktır. Çözüm, savunmasız dosyaları ve yazılımları koruyabilmeli ve aynı zamanda fidye yazılımının herhangi bir dosyayı şifrelemesini engellemelidir. Bir sonraki adım zaman ve çaba gerektirir. Verilerin düzenli olarak yedekleri oluşturmalı ve bunların harici bir ortamda depolanması sağlanmalıdır. Uzmanlar, yedeklemelerin şifreleme ve çok faktörlü yetkilendirme ile korunan bulut tabanlı bir çözümde depolamanızı önermektedir. Diğer bir seçenek de yedeklemeleri USB sürücüler veya sabit diskler gibi harici ortamlarda saklamaktır. Ancak, yedeği aldıktan sonra bunların bağlantılarının kesildiğinden emin olunmalıdır. Aksi takdirde, fidye yazılımının bu harici cihazlara da bulaşma ihtimali yüksektir. Sonraki adım, işletim sisteminizin ve diğer yazılımların güncel olmasını sağlamaktır. Popüler WannaCry fidye yazılımı, Microsoft işletim sistemindeki bir güvenlik açığından yararlandı. Microsoft, Mart 2017'de güvenlik açığını düzeltmek için bir güncelleme yayınladı ancak çoğu kişi bu güncelleştirmeyi görmezden geldi ve indirmedi. Bu, sistemlerin saldırıya açık hale gelmesine sebep oldu. İşletim sistemini ve diğer yazılımları manuel olarak güncellemenin zor olduğu, bu nedenle işletim sistemi ve diğer yazılımlar için otomatik güncellemelerin etkinleştirilmesinin en güvenilir olduğu anlaşılmaktadır.

Fidye yazılımı dağıtmak için kullanılan en yaygın teknik sosyal mühendisliğidir. Herkes kötü amaçlı web sitelerini, malspam'ı ve diğer zararlı yazılımları nasıl tespit edeceği konusunda eğitilmelidir. Her zaman içgüdülerinize güvenin. Bir şey zararlı görünüyorsa, kesinlikle öyledir.

5.1.6 Dosyasız Kötü Amaçlı Yazılım

Bu gerçekten kötü amaçlı bir yazılım türü değildir. Ancak kötü amaçlı yazılımın, bir kullanıcıyı istismar etmek için kullanılma biçimine dayalı olarak yapılmıştır.

Geleneksel kötü amaçlı yazılım, dosya sisteminin kontrolünü ele geçirerek sistemlere bulaşmaktadır. Diğer yandan, dosyasız kötü amaçlı yazılım ise dosya sistemine dokunmaz, ancak sistem belleğine yayılır veya API'ler (Application Program İnterface) , zamanlanmış görevler ve kayıt defteri anahtarları gibi dosya dışı diğer bileşenleri kullanmaktadır. Dosyasız kötü amaçlı yazılım, sistemde çalışan bir programı alt süreci haline getirmek için kullanır veya Microsoft Windows tabanlı işletim sistemlerinde PowerShell gibi sistem araçlarını kullanmaktadır. Saldırganlar, tespit edilmesi zor olduğu için dosyasız kötü amaçlı yazılımlar kullanmaya başladılar. Örneğin, ‘’Operasyon Kobalt Kitty’’, altı ay boyunca PowerShells'e bulaşmak ve Asya şirketlerine saldırmak için popüler hale gelen dosyasız kötü amaçlı yazılımdır. Kötü amaçlı yazılım, hedef sistemlere hedefli kimlik avı e-postaları kullanılarak yerleştirildi.

5.1.7 Reklam Yazılımı ve Kötü Amaçlı Reklamcılık

Kötü amaçlı yazılımlara yalnızca reklam yazılımı biçiminde rastlanılmamaktadır. Adware, kullanıcının bilgisi olmaksızın ve çoğu zaman başka bir yazılımla birlikte bilgisayara yüklenen programlardır. Bir bilgisayara bulaşır ve istenmeyen reklamları göstermeye devam eder. Reklam yazılımı aracılığıyla görünen en yaygın reklamlar, kullanıcıları diğer ürünler için promosyonlar içeren web sitelerine yönlendirirler. Reklam yazılımı potansiyel olarak zararsızdır ancak çok can sıkıcı olabilmektedir.

Bu reklam yazılımlarıyla karıştırılmamalıdır. Ancak kötü amaçlı reklamcılık, kötü amaçlı dosyaları hedef sisteme göndermek için gerçek reklamları kullanırlar. Örneğin; bir saldırgan, web sayfasına kötü amaçlı bir reklam yerleştirmesi için bir web sitesine ödeme yapar. Bu reklamı tıklayan bir kullanıcı saldırganın web sitesine yönlendirilerek, kötü amaçlı yazılımı anında kendi sistemine indirecektir. Çoğu zaman, reklamlardaki kötü amaçlı yazılımlar herhangi bir kullanıcı etkileşimi olmadan yürütülmektedir. Bu teknik "by-download" olarak adlandırılır. Saldırganların, reklamlar aracılığıyla ‘’Spotify, Hepsiburada, Amazon’’ gibi daha büyük web sitelerine kötü amaçlı yazılım dağıtmak için ‘’Yahoo’’ gibi büyük reklam motorlarına saldırdığı durumlar olmuştur.

5.1.8 Casus Yazılım

Casus yazılım, saldırganlar tarafından insanların faaliyetlerini gözetlemek için kullanılan kötü amaçlı bir yazılımdır. Çoğunlukla bir ilişkideki ortaklar tarafından birbirlerini gözetlemek için kullanılır. Ancak saldırganlar aynı zamanda hedefin etkinliğini anlamak ve tuş vuruşlarını kaydetmek için casus yazılım kullanırlar. Casus yazılımların siber zafiyet kapsamında da kullanılması, sebep olduğu zararları gün geçtikçe artırmaktadır. ABD'de ''Federal Soruşturma Bürosu'' tarafından 2005 yılında 2000'den fazla firma ile yapılan bir araştırmada, bu şirketlerin %64'ünün bilgisayarlar ve casus yazılım ilişkili zafiyetlerden finansal zararlara maruz kaldığı belirlenmiştir. ''Federal Soruşturma Bürosu'' oluşan bu finansal kaybın yaklaşık 62 milyar ABD doları olduğunu açıklamıştır. Webroot, 2005 yılı boyunca 420 binden fazla web sitesinde casus yazılım tespit etmiştir. Casus yazılımlar bu kadar etkin ve yaygın olduğu için, bu konuda alınması gereken tedbirlerin ve yapılacakların belirlenmesi gerekmektedir. Casus yazılımlar, ilgili sisteme bulaştıktan sonra bulaştığı yerde arka planda işlevini sürdürmeye devam etmektedir. Fakat çoğu zaman, casus yazılım olgusunu dile getirmek bazı önemli ve genel belirtiler ortaya çıkarmaktadır.

Eğer;

●Kullandığınız bilgisayar başlamada başarısızlığa düşüyor ya da kısa zamanda durduk yere yavaşlama eğilimi gösteriyorsa,

●Web sayfalarında gezinirken sizin istemediğiniz web siteleri karşınıza çıkıyorsa,

●İnternete girmek istediğinizde sizin istediğiniz sayfa değil de sürekli reklam içerikli sayfalar geliyorsa,

●Tarayıcınızın yer imi yâda sık kullanılanlar bölümünde tarafınızca eklemediğiniz farklı web site bağlantıları ekliyse,

●Tarayıcınıza başlangıçta ayarladığınız web sitesi olan "Başlangıç Sayfası", sizin ayarlanmadığınız farklı bir web sitesine yönleniyorsa ve bu ayarı tarafınızca değiştirseniz de yine farklı web siteleri ortaya çıkıyorsa,

●Tarayıcınızda daha önce sizin tarafınızdan görmediğiniz yer imi varsa,

●Araç çubuğunuzda daha önce gözlemlemediğiniz bir uygulama simgesi varsa,

●Kullanmakta olduğunuz bilgisayarda bir işlem olmadığı zaman birden ortaya çıkan ve size hitap eden tanıtım sayfaları çıkıyorsa,

●Tarayıcınızda bazı tuşlar (örneğin bir web sayfası formu doldururken bir sonraki yazım alanına geçmek için kullandığınız sekme tuşu) kullanılmıyorsa,

●Kullanmakta olduğunuz bilgisayar çalışmakta iken bilgisayarınızın hard diski hareketliliğini gösteren ışık devamlı yanıp sönüyorsa,

●Kullanmakta olduğunuz bilgisayarda herhangi bir işlem olmadığı anda araç çubuğundaki ağ bağlantısını gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren ışıklar yanıp sönüyorsa,

●Bilgisayar kasasındaki dâhili CD-RW sürücüsü kendiliğinden açılıp kapanıyorsa,

●Bilgisayar ekranınıza durup dururken hata iletileri geliyorsa,

Sistemde çok büyük ihtimalle casus yazılım bulunmaktadır. Sistemine casus yazılımın bulaştığını bu tür bulgular sonucunda fark eden bir kullanıcının aklına gelen ilk soru "Acaba bu yazılım sistemime nasıl bulaştı?" olacaktır.

Sıradan bir tarayıcı casus yazılımları algılayıp, kaldırmanıza yardımcı olabilmektedir. Günümüzde kötü amaçlı yazılımları ve virüsleri birbirinin yerine kullanmak yaygın bir uygulamadır. Fakat bunlar aynı şeyler değildir. Aradaki fark, kötü amaçlı yazılımın ana terim olması ve virüsün bir tür kötü amaçlı yazılım olabilmesidir. Basit bir ifadeyle, bir virüs kötü amaçlı yazılım olabilir, ancak tüm kötü amaçlı yazılımlar bir virüs olmamaktadır. Bir ''Venn Diyagramı'' olarak temsil edilirse, aşağıdaki şekle benzeyecektir. Virüs, bir tehdidin alt kümesi olan kötü amaçlı yazılımın alt kümesidir.

Sistemde Virüs Veya Kötü Amaçlı Yazılım Olduğu Nasıl Anlaşılır? Bir virüs çoğunlukla bir dosyaya bulaşır ve kendisini diğer dosyalara çoğaltır. Bununla birlikte, virüs kötü amaçlı yazılım olarak dağıtıldıysa, en yaygın gösterge sisteminizin yavaşlaması olacaktır. Bazıları sabit sürücünüzdeki mevcut tüm depolama alanı dolana dek kendini çoğaltır ve bilgisayarınızı bir tuğlaya dönüştürür. Bazıları verilerinizi çalışmaz hale getirip, bilgisayarınızın stabilitesini bozmaktadır. Ve hatta bazıları

bilgisayarınızdaki kişi listesini kullanarak kendini başka bilgisayarlara da yaymaya çalışır. Tabii tüm bunların yanında yazılımın uzaktan erişim için bir altyapı kurabileceği de söylenebilir. Normal bir durum olarak kimse virüs bulaşmış bilgisayara sahip olmak istemez. Bu nedenle güvenilir alışkanlıklar edinmek ve bilindik antivirüs yazılımlarını kullanmak önemlidir. Neredeyse tüm kötü amaçlı yazılımlardan biraz dikkat ve biraz bilgi ile sakınılabilir. Antivirüs yazılımınız da güncelse bilgisayarınızın çok iyi durumda olduğu söylenebilir. Yine de çeşitli durumlarda bu kötü amaçlı yazılımlar savunmamızı aşabilir. Belki antivirüs yazılımınız güncel değildir ya da zekice hazırlanmış bir kod parçası ile atlatılmıştır. Belki de yanlışlıkla bir bağlantıya tıklanmıştır. Ya da başka birisi bilgisayarınızı kullanıp kötü amaçlı yazılımlar indirmiştir. Genellikle bir virüs söz konusu olduğunda antivirüs yazılımınız alarm durumuna geçip size bilgi verecektir. Ancak çeşitli durumlarda atlamalar olabilmektedir. Böyle bir durumda ilk olarak ‘’Bilgisayarınızda virüs olup olmadığını anlatan bir işaret var mı?’’ sorusu akla gelmektedir. Aslında, bilgisayarınızda kötü amaçlı yazılımların varlığını gösterebilecek birkaç işaret bulunmaktadır.

- Bilgisayarınızdaki çökmeler ve donmalar virüse işaret eder.
- Bilgisayarınızdaki sürücüye erişim engeli virüse işaret eder.
- Bilgisayarınızdaki kaybolan dosyalar virüse işaret eder.
- Bilgisayarınızdaki sizce yüklenmeyen programlar virüse işaret eder.

5.2 Antivirüs Ve Kötü Amaçlı Yazılımdan Korunmak Gereklimi?

Bugün, virüsten koruma ve kötü amaçlı yazılımdan koruma çözümleri aynı şeydir. Hiçbir sağlayıcı yalnızca virüsleri kontrol etmez. Solucanları, truva atları, fidye yazılımları gibi diğer kötü amaçlı yazılımları taramayan bir çözüm sunmazlar. İyi bir güvenlik çözümü, sistemdeki yerel dosyaları tarayacak ayrıca e-posta ve internette gezinme yoluyla çevrimiçi etkinlikleri gözlemleyecektir. Kötü niyetli bir web sitesine ziyarette bulunursanız güvenlik çözümü tarayıcının yüklenmesine izin vermeyecektir.

5.3 Kötü Amaçlı Yazılımlardan Koruma

Sisteminize virüs bulaştığı düşünülüyorsa yapılması gereken birkaç şey vardır. Bunlar bazıları şu şekildedir:

5.3.1 Antivirüsünüzü Kurun / Güncelleyin

Bir antivirüs çözümü yok ise, bir tane satın alınmalı ve hemen kurulmalıdır. Sisteminizin sağlığı ve içerdiği önemli veriler için ödenmesi gereken küçük bir bedeldir. Diğerlerinin yanı sıra ‘’Norton Security, Kaspersky, McAfee ve Avast’’ gibi sağlayıcılara genellikle güvenilmelidir. Bu çözümlerin çoğu 4,5 yıldızla derecelendirilmiştir. Virüsten koruma yazılımını yükledikten sonra derinlemesine bir tarama yapılmalı ve çok zaman alsa bile çalışmasına izin verilmelidir. Tek sorun, kötü amaçlı yazılımın çok gelişmiş olmasıdır, antivirüsün nasıl devre dışı bırakılacağını bilir. Zaten bir antivirüs çözümünüz varsa ve kötü amaçlı yazılımı tespit edemediyse, bu çoğunlukla programı güncellemediğiniz anlamına gelmektedir. Bu süreç yalnızca bir antivirüs çözümü yüklenerek bitmez. Her gün yeni kötü amaçlı yazılım geliştirilir. Bu nedenle, yeni kötü amaçlı yazılımı algılayabilmeleri için antivirüs programlarının güncellenmesi gerekmektedir. Virüsten koruma yazılımı güncellenmediğinde bir gün bile geçse sistemi yeni kötü amaçlı yazılımlara açık hale getirilmiş olunur.

5.3.2 Sistem Geri Yükleme

Microsoft Windows gibi çoğu işletim sistemi, sistem geri yükleme adı verilen bir özelliğe sahiptir. Bu, temel olarak tüm sistemin bir yedeğini düzenli aralıklarla depolamaktadır. Sisteme bugün kötü amaçlı yazılımlar bulaştıysa ve dün için kullanılabilir bir sistem geri yükleme noktası varsa, sistem dün olduğu gibi geri yüklenebilmektedir. Bu da kötü amaçlı yazılımı kaldıracağı anlamına gelmektedir. Ancak bazen kötü amaçlı yazılım kodu, sistem geri yüklemesini çalıştırılmasına izin vermeyecek şekilde yazılır. Bu gibi durumlarda, güvenli modu etkinleştirmek için sistemin yeniden başlatılması ve ardından bir sistem geri yükleme noktası çalıştırılması gerekmektedir.

5.3.3 İnternet Bağlantısını Kesin

Sistemde bilgi çalmak için kullanılan kötü amaçlı yazılım varsa, bu birisinin İnternet üzerinden onu uzaktan kontrol ettiği anlamına gelmektedir. Bununla başa çıkmanın ilk adımı İnternet bağlantısını tamamen kesmektir. Ethernet kablosunu çıkarılmalı, Wi-Fi devre dışı bırakılmalıdır. Hatta gerekirse modem kapatılmalıdır. İnternet bağlantısı kesildiyse antivirüs güncellenmeyeceği iddia edilmektedir. Antivirüs bir çevrimdışı-offline çözüm yoluyla yüklenmelidir. En azından, saldırgan artık bilgisayara, tablete, erişemeyecektir.

5.3.4 Taşınabilir Bir Antivirüs Çözümü Edinin

Her şey başarısız oluyorsa ve antivirüs kurmanıza bile izin verilmiyorsa, bu kötü amaçlı yazılımın işletim sisteminin kontrolünü ele geçirdiği anlamına gelmektedir. İşletim sistemiyle uğraşmak zorunda kalmadan kontrolü ele almanın bir yolunun bulunması gerekmektedir. Bu gibi durumlarda, bir USB sürücüsüne yüklenebilen, taşınabilir offline-çevrimdışı antivirüs çözümleri kullanılmalıdır. Bunlardan bazıları ‘’ClamWin, Kaspersky Security Scan, McAfee Stinger ve Microsoft Safety Scanner'dır.’’ Aslında, bunların tümü bir USB sürücüsünde tutulabilir ve herhangi bir çakışmaya neden olmadan ayrı taramalar yapılabilmektedir. Kötü amaçlı yazılımın bulaşmasının sonucu tekrar başlangıç da zor olacaktır. Soyulmuş bir evde yaşamak için geri dönmek gibi nitelendirilebilmektedir. Tekrar güvende hissetmek zaman alacaktır. Sistem geri yüklendiğinde, sistemin güvenliğini artırmak için adımlar atılmalıdır. Biraz maliyetli olsalar bile en iyi güvenlik çözümleri satın alınmalıdır. Ayrıca, istenmeyen yazılımlar düzenli aralıklarla kaldırılmalı ve geçici dosyalar silinmelidir. Bu süreçten sonra daha titiz ve dikkatli olunmalıdır.

6 BİR SOSYAL MÜHENDİSLİK SALDIRISI NASIL TESPİT EDİLİR VE DURDURULUR

Sosyal Mühendislik, insanları size onlar hakkında ihtiyacınız olan bilgileri vermeleri için manipüle etme veya kandırma sürecidir. Siber suçlular her türlü bilgiyi ararlar,

ancak en yaygın olanları, banka bilgileri, çeşitli uygulamalara giriş kimlik bilgileridir. Bilgisayarınıza erişmek ve şifrelerinizi ifşa etmeye ikna etmek için sosyal mühendislik kullanırlar. Bu bilgileri, kendi hesaplarınızdan kendi hesaplarına para aktarmak veya sisteminize kötü amaçlı yazılım yüklemek için kullanırlar. Siber suçlular; sosyal mühendisliğin, bir kişinin güvenini kazanmanın bilgisayara fidye yazılımı yüklemekten daha kolay olduğunu bilirler. Örneğin, herhangi bir kurbanı şifresini vermek üzere manipüle etmek için basit konuşmaları kullanırlar. Bir şifre veya başka bir teknik işlem kullanarak sistemi hacklemeye çalışmazlar. Kullanıcının zayıf bir şifresi varsa sisteme saldırabilirler. Güvenliğin temel ilkesi kime ve neye güvenileceğini bilmektir. Bir kişiye ne zaman güvenileceğini bilmeli ve onlarla iletişim kurduğunuzda, göz teması kuramayacağınız için uyanık olmak gerekir. Bu, güvenilen uygulamalar için de geçerlidir. Sisteminize veya web sitenize indirip yüklediğiniz bir uygulamanın orijinal olup olmadığını ve size zarar verip vermeyeceğini bilmeniz gerekmektedir.

Herhangi bir güvenlik uzmanı, işletmelere, bir güvenlik zincirindeki en zayıf halkanın, başka bir kullanıcıyı itibari değerde kabul eden ve ona güvenen bir kullanıcı olduğunu söylemektedir. Basit bir deyişle, eviniz için çoklu kilitler, bekçi köpekleri, projektörler, alarm sistemleri, dikenli teller, çitler vb. ile birinci sınıf güvenliğinizin olması fark etmez. Eğer bir yabancının sadece tesisatçı olduğunu iddia ettiği için evinize girmesine izin verirseniz, herhangi bir kontrol yapmadan evinize girme tehdidi güçlendirilmektedir.

6.1 Sosyal Mühendislik Metodolojileri

Sosyal mühendislik için kullanılan üç tür metodoloji vardır:

● Kimlik avı

● Vishing

● Kimliğe Bürünme

Kimlik Avı ve Vishing, daha önce ayrıntılı olarak önceki bölümlerde anlatılmıştı. Ancak, ‘’Kimliğe Bürünme,’’ bir saldırganın zaten tanıdığınız biri gibi davranarak ve sizi kandırarak bilgisayarınıza, ağınıza vb. erişim sağlamasıdır. Saldırgan, kimliğe

bürünme tekniğini hesaplarınızı ve sistemlerinizi hacklemek için kullanmadan önce çok fazla araştırma yapar. Saldırganlar, insanları sosyal medyada ve şirket web sitelerinde takip eder ve kurbanın arkadaşları ve meslektaşları hakkında bilgi toplarlar. Ayrıca konuşmalarınızı dinler ve çöpe attığınız belgeleri incelerler.

6.2 Bir Sosyal Mühendislik Saldırısını Tespit Etme

Bir sosyal mühendislik saldırısının genellikle nasıl yapıldığını anlamak zor değildir. Sosyal mühendisliğin nasıl çalıştığını anlamak için bazı yaygın senaryolar vardır.

6.2.1 Bir Arkadaştan E-posta

Saldırgan, bir kullanıcının e-posta şifresini yazılım veya sosyal mühendislik yoluyla ele geçirmeyi başarırsa, o kullanıcının kişi listesine erişebilir. Çoğu kullanıcının çok sayıda web uygulaması veya sosyal medyası için aynı şifreyi kullandığı bilinmektedir. Saldırgan kullanıcının sosyal medyasına ve sosyal medyadaki kişilerine de erişebilir. Bundan sonra her şey saldırgan için kendi alanıdır. Kullanıcının kişi listesine e-postalar veya sosyal medyadan anlık mesajlar gönderebilir. Saldırgan tarafından gönderilen mesajların çoğu aşağıdaki özelliklere sahiptir;

● Saldırgan arkadaş gibi davranarak, ilgili olabileceğiniz bir şey söyleyip sizi heyecanlandıran bir URL'den bahsedebilir. Size bir bağlantı gönderebilir ve bu bağlantı aracılığıyla sizden bazı bilgiler vermenizi isteyebilir. Şüphesiz ve masum. Çünkü bir tanıdığınızdan geliyor. Bağlantıya tıklanıyor ve bilgisayara bulaşan kötü amaçlı yazılımlar indiriliyor. Artık sisteme erişebilir ve istediği herhangi bir işlemi gerçekleştirebilir. Saldırganlar kişi listenizdekiler hakkında bilgi toplamaya ve sizi aldattıkları gibi onları da aldatmaya çalışacaklardır. Türkiye'de sosyal medya mesajlaşmalarında genellikle ''Hediye çeki dağıtıyorum.'' yalanıyla telefon numarası istenmekte ve bu sayede kişiler dolandırılmaktadır.

● Dosya içeriğine kötü amaçlı kod parçacığı gizlenmiş bir görüntü, video veya müzik dosyası olduğu bir mail yollanmıştır. Dosya bir arkadaşınızdan geldiği için tereddüt etmeden indirilir ve sonunda sisteminize kötü amaçlı yazılım bulaşmış olur. Saldırganın artık bilgisayarınıza ve üzerinde bulunan verilere erişimi vardır.

Bu tip saldırılardan korunmak için tüm sosyal medya şifrelerinin aynı yapılmaması gerekmektedir. Her biri için ayrı ve güçlü parola belirlemek daha güvenli olacaktır. Eğer yapılabiliyorsa two faktör güvenlik önlemi alınmalıdır. Bu sayede saldırgan sadece sınırlı sayıda kitleye ulaşacaktır. Kimden gelirse gelsin yakın akrabalarınızdan bile olsa gönderdikleri dosyayı bilgi almadan indirmemeli veya farklı bir işlem yapmamalıdır.

6.2.2 Güvenilir Bir Kaynaktan Bir E-posta

Sosyal mühendislik, saldırganların hassas bilgileri ifşa etmek, kullanıcıları kandırmak için güvenilir bir kaynağı taklit ettikleri kimlik avı saldırısıdır. Webroot'tan gelen raporlar, çoğu saldırganın finansal kurumların kimliğine büründüğünü gösteriyor. Verizon'dan gelen veriler, bugün meydana gelen ihlallerin %93'ünün başarılı bir sosyal mühendislik girişiminin sonucu olduğunu da göstermektedir.

Güvenilir kaynaklardan gelen e-postalar aşağıdaki temalara sahip olabilir;

● E-postalar acil yardım isteyebilir. Bazı e-postalarda acil mesajlar olabilir ve aciliyet duygusu sizi e-postadaki eylemi yapmaya zorlayabilir. Korktuğunuz için, parayı saldırganın hesabına aktarabilirsiniz.

● E-posta, bir amaç için bağış isteyebilir. E-postalar cömertliğinizi veya nezaketinizi istismar etmeye çalışabilir. İçerik, bir vakfa veya amaca yönelik bir miktar fon aktarmanız gerektiğini söyleyebilir, ancak para doğrudan saldırganın hesabına gitmektedir.

● Gerçek bir arka plan kullanan kimlik avı girişimleri. Bir saldırgan size para göndermenizi isteyen bir mesaj veya e-posta gönderebilir. Mesajın veya e-postanın kaynağı tanınmış bir şirket, okul veya kurum olabilir izlenimi verilebilir.

● E-posta bir sorun olduğunu söyleyecek ve düzeltmek için bir bağlantıya tıklamanızı isteyecektir. E-postayı göndermek için kullanılan URL gerçekmiş gibi görünebilir. E-postanın gövdesinde saldırganın aitmiş gibi davrandığı kuruluşa benzer bir logo kullanılabilir. Saldırganın e-postayı doğrudan kaynak web sitesinden göndermesi, ancak bu web sitesine erişmek için farklı yöntemler kullanması mümkündür. Her şey yasal göründüğünden, sizi saldırganın web sitesine yönlendiren URL'ye

tıklayabilirsiniz. Saldırgan, hesabınıza girmek için ihtiyaç duyduğu bazı bilgileri isteyen bir form sunacaktır. E-posta ayrıca, URL'yi tıklamazsanız sonuçların ne olabileceğini söyleyen bir uyarı da içerir. Bunun amacı sizi korkutarak bağlantıya tıklamanızı sağlamaktır.

Yöneticiniz veya meslektaşınız gibi davranmak: E-posta, ofisinizde üzerinde çalıştığınız bir projenin ayrıntılarını içerebilir. Bu güveninizi kazanmak için yapılmış bir harekettir. Bir sonraki bölüm, geçmişte yapmış olduğunuz bir şirket kartını kullanarak bir tür ödeme ile ilgili olacaktır. Bunun doğru olduğuna inanıyorsunuz ve ödemeyi yapıyorsunuz.

Sana bir şey kazandığını söyleyen bir posta: Ölen bir akrabanızdan, bir piyango şirketinden veya başka herhangi bir işletmeden e-posta almış olabilirsiniz. Bazı e-postalar, web sitesini ziyaret eden 100. kişi olduğunuzu ve bir şey kazandığınızı da söyleyebilir. E-posta, kim olduğunuzu kanıtlamak için sosyal güvenlik numaranız gibi bazı hassas belgeler sağlamanızı ister. Bu istekler sizi şüpheli kılmalıdır. E-postalara güvenmeyin. Bu tür saldırı, açgözlülük kimlik avı olarak bilinir. Açgözlü olduğunuz için saldırgana gerekli bilgileri vermek isteyebilirsiniz. Sonuç olarak, saldırganın banka hesabınızı boşaltmak için kullanabileceği hassas bilgileri ona sunmuş olabilirsiniz.

Ücretsiz filim ve müzik indirme: Bu sosyal mühendislik senaryosunda, saldırganlar, özellikle hassas bilgiler elde etmek istiyorlarsa kullanıcıyı tuzağa düşürebileceklerini bilirler. Bu tür yemler genellikle ücretsiz filmler veya müzik indirmeleri sunan web sitelerinde bulunur. Saldırganlar bu tür dolandırıcılıkları kötü amaçlı web sitelerinde, sosyal medyada ve çoğu kullanıcının arama sonuçlarında rastladığı diğer web sitelerinde çalıştırabilir.

Tuzak planı; bir telefon satmayı teklif eden bir web sitesinde de ortaya çıkıyor: Gerçek maliyeti 1.000 TL olan telefon için sizden yalnızca 100 TL istenmiş olması dikkat düşündürücüdür. Şüphelenebilirsiniz, birçok kullanıcıdan teklifin doğru olduğunu ifade eden yorumlar yapılmış gibi gösterilmektedir. Saldırgan bunu şüphelerden uzak olunması için zekice tasarladı. Bu yemlemeden hoşlanan kullanıcılar bilgisayarlarına kötü amaçlı yazılım indirir. Bu sayede kullanıcı hakkındaki ayrıntıları ve iletişim

kurduğu diğer kullanıcılar hakkındaki diğer verileri ortaya çıkarır. Onlara 100 TL ödeyebilirsiniz, ancak karşılığında vaat edilen telefonu asla alamazsınız.

Sormadığınız Soruları Yanıtlamak: Saldırganlar, bazen bir şirketten avantajlar sağlamak ve yardım etmek için sizinle iletişime geçerler. Size gelen E-posta kimliği, tanınmış bir şirket veya bankaya benziyor olabilir. Ürünün tüketicisi değilseniz, e-postayı silersiniz. Ancak, ürünü kullanıyor olma ihtimaliniz yüksektir. Aslında yardım için şirketle iletişime geçmeniz planlanıyordur. Örneğin, işletim sisteminizdeki bir sorunla ilgili yardım istenmiş olunabilir, ancak aniden Microsoft'tan bir e-posta gelir. E-posta, sorunu ücretsiz olarak çözmeyi teklif etmektedir. Onlara yanıt verirseniz ve onlara güvenirseniz, kendinizi saldırganın önceden planladığı çeşitli istismarlara açmış olursunuz. Saldırgan sizden kimliğinizi doğrulamanızı, sistem veya uygulamada oturum açmak için gerekli bilgileri sağlamanızı isteyecektir. Diğer zamanlarda, sorunu çözmek için sisteminizde birkaç komut çalıştırmanız istenebilir. Bunu yapmalarına izin verdiğinizde, sisteminize erişirler.

Güvensizlik Yaratma: Bazı sosyal mühendislik uygulamaları yalnızca güvensizlik veya çatışmalar yaratmak için uygulanır. Bunlar tanıdığınız ve sorun yaşayan kişiler tarafından ya da dünyanın yanmasını izlemekten zevk alan kişiler tarafından yapılır. Bu saldırganlar, kafanızı tanıdığınız diğer insanların yanlış izlenimleriyle dolduracak ve ardından güveninizi kazanmak için kurtarıcı olarak gelecektir. Bu tür kötü uygulamalar, başlangıçta sizi manipüle etmek ve daha sonra size saldırmak isteyen gaspçılar tarafından da kullanılır. Bu tür bir sosyal mühendislik saldırısı hesaplarınızdan birine erişim sağlayarak başlatılır. Bu, şifrenizi kırarak, sosyal mühendislik yaparak veya sadece şifrenizi tahmin ederek elde edilebilir.

Artık sosyal medyanıza, videolara ve resimler gb uygulamalara erişimi olan saldırgan, bunları ihtiyaçlarına göre düzenler ve güvensizlik ortamı yaratmak için kişilerinize iletebilir. İçeriği yanlışlıkla iletildi gibi davranırlar. Saldırgan, çalınan medya içeriğini saldırıya uğrayan kullanıcıya şantaj yapmak için de kullanabilir.

Sosyal mühendislik saldırılarının birçok çeşidi vardır. Saldırganın hayal gücü, birisini sömürme yöntemlerinin tek sınırıdır. Tek bir saldırı, birden fazla sayıda istismar içerebilir. Saldırgan, daha sonra istismar edilebilmeniz için bilgilerinizi sizden hoşlanmayan kişilere para karşılığı satabilir.

6.3 Sosyal Mühendisliğe Düşmekten Nasıl Kaçınılır?

Bir sosyal mühendislik saldırısının raf ömrü kısadır ve başarılı olması için sadece birkaç kullanıcıya ihtiyacı vardır. Ancak kendinizi buna karşı koruyabilirsiniz. Çoğu zaman çevrenizden haberdar olmanız gerektiğinden çok fazla çaba gerektirmez.

6.3.1 Ağırdan Almak

Bazı saldırılar karşısında durmak ve biraz düşünmek iyi bir fikirdir. Saldırganlar, düşünmeden acilen hareket etmenizi beklemektedirler. Çoğu sosyal mühendislik saldırısı sizi acil görünen bir duruma sokar. Bu, durumu doğru bir şekilde yavaşlatmak ve gözden geçirmek için ipucunuz olmalıdır.

6.3.2 Araştırmaya Biraz Zaman Harcayın

Bildiğiniz birinden veya güvendiğinizi düşündüğünüz bir işletmeden e-posta alabilirsiniz. Sadece e-postanın gövdesi değil, aynı zamanda "gönderen" adresi, imzası vb. iyice gözden geçirilmelidir. Şirketi tanımıyorsanız, gerçekten var olup olmadıklarını görmek için basit bir araştırma yapılmalıdır.

6.3.3 Bağlantılara Körü Körüne Tıklamayın

E-postada bir bağlantı alırsanız, bağlantıya tıklamayın. Bir arama yoluyla bu web sitesi URL'sini bulmak için biraz çaba sarf edin ve temel URL'nin sizi nereye götürdüğünü görün. Bu şekilde, bağlantının kontrolü sizde olacaktır. Bunun tersi olması durumunda araştırılmadan tıklanan linkler, kötü niyetli kişilerin amaçlarına ulaşmalarını sağlayacaktır.

6.3.4 E-posta Hack'lerinin Farkında Olun

Saldırganlar e-posta hesaplarını ele geçirir ve saldırıya uğramış hesabın kişi listesindekilerin güvenlerine dayanarak saldırıda bulunurlar. Bu nedenle, tanınan birinden bir e-posta alındığında, bu mailin beklenip beklemediğinin sorulması gerekmektedir. Postayı beklemediyseniz postadaki herhangi bir bağlantıya tıklamayın.

Kişiyi aramak ve size postayı gerçekten gönderip göndermediğini doğrulamak güvenli bir seçenektir.

6.3.5 Körü Körüne İndirme

Göndereni tanımıyorsanız, e-postadaki hiçbir eki indirmeyin. Eklerin ne olduğuna özellikle dikkat edilmelidir. Uzantılarına bakılmalı exe, pdf ya da makro çalışacak, çalışabilme ihtimali olan hiçbir ek indirilse bile çalıştırılmamalıdır.

6.3.6 Piyangoların Sahte Olduğunu Bilin

Kimse size bedavadan bir sürü para vermiyor. Yani, bir e-posta alırsanız özellikle herhangi bir yarışmaya katılmadan bir şey kazandığınızı söylemek bir aldatmacadır. Klasik bir örnek, Harry Potter ve Zümrüdüanka Yoldaşlığından Tonks'un Dursley'lere en iyi çim için bir yarışma kazandıklarını söyleyen bir mektup gönderdiği sahnedir. Bunu sadece Dursley'ler Harry'yi Kovuk'a götürmeye çalışırken yollarına çıkmamaları için yaptı. Böyle bir e-posta alırsanız sahtedir ve tedbirli olunması gerekmektedir.

6.3.7 Banka Dolandırıcılıklarına Dikkat Edin

Size gelen bir e-posta kişisel bilgilerinizi ve banka bilgilerinizi soruyorsa, büyük olasılıkla bir dolandırıcıdır. Bu e-postayı silin, ayrıca bu gönderenden gelecek tüm e-postaları almamak için bir filtre oluşturun.

6.3.8 Yardım Tekliflerini Reddet

Gerçek şirketler sizinle proaktif olarak iletişime geçmezler. Herhangi birinden e-posta alırsanız, sohbeti başlatmadığınızda, özellikle aşağıdakileri yapabileceklerini söylerlerse bu bir aldatmacadır:

- Kredi puanınızı iyileştirmenize yardımcı olmayı teklif eder.
- Sisteminizdeki bir uygulamayı veya yazılımı düzeltmeyi teklif eder.

Bir hayır kurumundan tanımadığınız bir e-posta veya mesaj alırsanız silinmelidir. Bir hayır kurumuna gerçekten bağış yapmak istiyorsanız, biraz araştırma yaparak meşru bir hayır kurumuna bağışta bulunulmalıdır.

6.3.9 Spam Filtrelerinizi Yapılandırın

İstenmeyen posta filtreleri, e-postaları meşru veya istenmeyen posta olarak sınıflandırmanıza yardımcı olan bir özelliktir. Biraz zaman ayrılmalı ve spam filtreleri güncellenmelidir. Yalnızca istenilen e-postalara izin vermek için kurallar belirlenmelidir. E-posta sağlayıcınız aracılığıyla istenmeyen posta filtrelerinizi nasıl ayarlayacağınıza dair kılavuzlar vardır. Otuz dakika kadar kısa bir zaman ayırımı, "e-posta hayatınızı" sonsuza kadar kolaylaştıracaktır.

6.3.10 Tüm Cihazlarınızı Koruyun

Tüm cihazlara virüsten koruma ve kötü amaçlı yazılımdan koruma programları yüklenmelidir. Yazılım rutin bir tarama yapacak şekilde ayarlanmalıdır ve gelen herhangi bir e-posta için gerçek zamanlı taramalar çalıştırmalıdır. Otomatik güncelleştirmeleri etkinleştirerek işletim sisteminin ve diğer yazılımların güncel tutulması sağlanmalıdır.

7 UYGULAMA

Siber saldırılarda insan faktörü ve zafiyeti daima ön planda olmuştur. Alınan ve alınması gereken tedbirler ve bu tedbirlerin uygulanması, denetlenmesi veri güvenliği için son derece önemlidir. Kişisel verilerin çalınması, sızdırılması ya da kritik öneme haiz bilgi ve belgelerin zafiyete uğraması tüm otoriteler tarafından asla kabul edilemez bir olaydır. Sızdırılan bilgi ve kişisel veriler yanında önemli ölçüde prestij ve para kayıplarına neden olmaktadır. Siber saldırılardan korunmak için ilk önce siber saldırıların nasıl gerçekleştirildiğinin bilinmesi ve bu yöntemlerin incelenmesi en önemli hususlardandır. Siber saldırı modellemeleri nasıl yapılır ve nelerden yararlanılır hangi araçlar ve hangi açıklıklar kullanılır bu hususlara hakim olmak ve bilmek zafiyetleri en aza indirecektir.

Siber saldırıların başlangıcı ilgili yer ile ilgili veri toplama ile başlar. Toplanan veriler doğru araç kullanımı ile etkin bir saldırıyı tetikler. Etkin bir saldırı toplanan verilerin ışığında siber zafiyetleri beraberinde getirmektedir. Birçok saldırgan birinci öncelik olarak Linux sistemlerini ve araçlarını etkili bir saldırı aracı olarak kullanmaktadır.

Burada amacımız bir siber zafiyetin nasıl gerçekleştirildiğinin ve bilgi toplama araçlarının nasıl kullanıldığının etkin bir biçimde kullanılarak bu yöntemleri gözler önüne sermektir. Ayrıca tarama araçlarını kullanarak zafiyet içeren portları ve diğer açıklıkları tespit etmek, bu portların açıklarından faydalanılarak ilgili zafiyetleri kullanarak sistemin nasıl zafiyete uğratıldığını göstermektir. Bilgi toplama araçlarından NMAP ve Essential NetTool kullanılmıştır. Bu araçlar etkili ve aktif olarak kullanılmaktadır. Bu saldırıları gerçekleştirmek için öncelikle her zaman bir IP adresine veya IP aralığına ihtiyaç duyulmaktadır. Bu nedenle bu araçlar bu IP adreslerini kullanarak açıklıkları tespit etmektedir. Hedef belirleme en basit yöntemiyle CMD (Command) ekranı ile ilgili web sitesine ping atarak bulunmaktadır. Ping www.google.com yazdığımızda Google sunucusunu IP adresi çıkmaktadır. Bu yöntemle belirli sayfalara atak düzenlemek için ilk kaynak olan IP adresine ulaşılmaktadır. Aynı şekildeki ağda bulunan diğer bilgisayarlarında IP leri bu şekilde bulunmaktadır. Essential NetTools ya da farkı programlar aracı aynı ağda kullanılan IP bloğu aralığı yazılarak aktif olan bilgisayarlar belirlenerek ilgili araçlar ile saldırılar düzenlenmektedir.

Uygulamada bir zafiyetli bilgisayara NMAP yardımı ile tarama yapılarak port açıklıkları belirlenecektir. Bu ataklar için Kali Linux ve araçları kullanılacaktır. Hedef IP ler bağlı bulunulan ağda taranacak ilgili portlar incelenecektir. Açık olan portlara göre hangi atakları düzenleneceği değerlendirilecektir. Bu açıklıklar çoğunlukla insan zafiyeti yüzünden ya da kullanılan bir uygulama için açık bırakılan portlardır. Bu portların kullanılmıyorsa belirli zamanlarda taranarak kapatılması, kullanılıyorsa da ilgili zafiyetler için tedbirlerin alınması gerekmektedir. Essential NetTool ile yine public IP taraması yaparak kullanılan modemlere ya da güvenlik kameralarına atak düzenlenmektedir. Ataklar gerçek zamanlı kullanılan IP bloklarına ve cihazlara yapılacaktır. Bu ataklar insan zafiyetini gözler önüne sermek için yapılmıştır. Bu atakların bertaraf edilmesi için fabrika çıkışı (default) şifrelerin değiştirilmesi gerekmektedir.

7.1 NMAP Nedir?

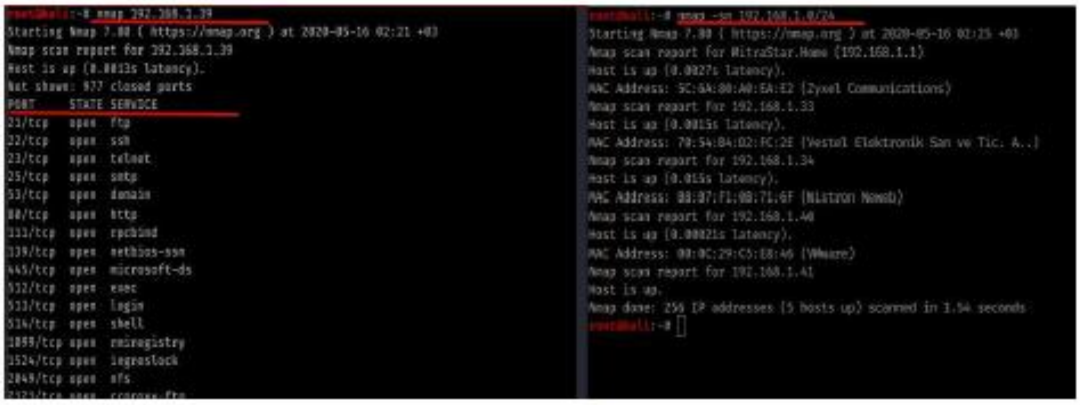
Nmap (“Network Mapper”), ağdaki farklı bağlantı noktalarını (port) tarayarak güvenlik açıklarını bulmak için kullanılan açık kaynaklı bir yazılımdır. Nmap ile bir

hedef sistemin ağ haritasını çıkartılarak, hedef sistemlerde hangi cihazların çalıştığını belirlemek, mevcut ana bilgisayarları ve sundukları hizmetleri keşfetmek, açık bağlantı noktaları bulmak ve güvenlik risklerini tespit etmek için de kullanılır. Nmap yapılan isteklerden gelen yanıtları dinler ve bağlantı noktalarının bir güvenlik duvarı tarafından açık, kapalı filtrelenmiş olup olmadığını belirleyebilir. Kurumsal ölçekli ağlar için geliştirilmiştir ve binlerce bağlı cihazı tarayabilir.

Hedef Belirleme

• Nmap'in en temel işlevlerinden biridir. Ağınızdaki etkin ana bilgisayarları tanımlamak için ping taraması yapılması gerekmektedir. Bunun için ilgili IP bloğunu girilir. Ping taramasını –sn parametresi kullanarak gerçekleştireceğiz. Bu parametre bağlantı noktası taramadan IP taraması yapacaktır. Bunu için kullanılacak parametre: nmap -sn 192.168.1.0/24

• Sadece belli bir IP adresi taraması gerçekleştireceksek nmap 192.168.1.1 gibi parametre girilir. Bu ilgili IP de açık olan portları ve servisleri listeleyecektir. Host taramak içinde aynı şekilde nmap Google.com gibi taramalar gerçekleştirilebilir. İlgili parametreler ile örnekler aşağıda gösterilmektedir.



Şekil 7.1 : Nmap Nedir

• Belirli bir IP aralığını/bloğunu, bağlantı noktası taramayı devre dışı bırakarak, yalnızca ana bilgisayarları bulmak için nmap 192.168.1.0/24 –sn parametresi kullanılır.

• Bir dosyadan hedefleri taramak için nmap - iL targets.txt parametresi kullanılır.

7.2 NMAP Tarama Teknikleri

Nmap kullanarak bağlantı noktası taraması yapmanın birkaç yolu vardır. En yaygın olarak kullanılanlar:

• sS TCP SYN scan

• sT TCP connect scan

• sU UDP scans

• sY SCTP INIT scan

• sN TCP NULL Bu tür taramalar arasındaki en büyük fark TCP veya UDP bağlantı noktalarını kapsayıp kapsamadıkları ve bir TCP bağlantısı yürütüp yürütmedikleri. Temel farklılıklar şunlardır:

• Bu taramalardan en temel olanı -sS TCP SYN taramasıdır ve bu çoğu kullanıcıya ihtiyaç duydukları tüm bilgileri verir. Saniyede binlerce bağlantı noktasını tarar ve bir TCP bağlantısını tamamlamadığından şüphe uyandırmaz.

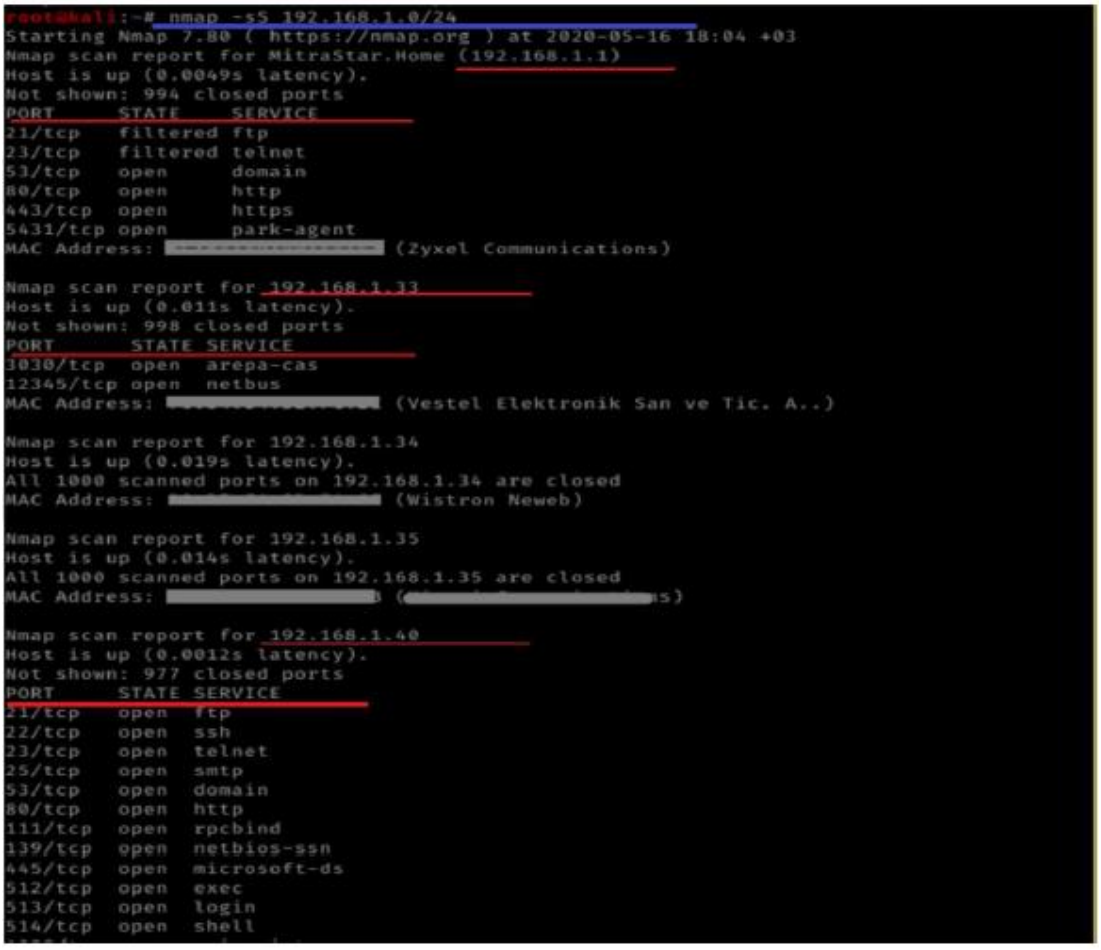
• Bu tarama türünün ana alternatifi, her ana bilgisayarı etkin bir şekilde sorgulayan ve yanıt isteyen TCP Connect taramasıdır. Bu tür tarama bir SYN taramasından daha uzun sürer, ancak daha güvenilir bilgiler döndürebilir. –sT

• UDP taraması TCP bağlantı taramasına benzer şekilde çalışır, ancak DNS, SNMP ve DHCP bağlantı noktalarını taramak için UDP paketleri kullanır. Bunlar, bilgisayar korsanları tarafından en sık hedeflenen bağlantı noktalarıdır ve bu nedenle bu tür tarama, güvenlik açıklarını kontrol etmek için yararlı bir araçtır. -sU

• SCTP INIT taraması farklı bir hizmet grubunu kapsar: SS7 ve SIGTRAN. Bu tür bir tarama, tüm SCTP işlemini tamamlamadığı için harici bir ağı tararken şüpheyi önlemek için de kullanılabilir. –sY

• TOP NULL tarama aynı zamanda çok kurnaz bir tarama tekniğidir. TCP sisteminde, bağlantı noktalarını doğrudan sorgulamadan gösterebilen bir boşluk kullanır, bu da bir güvenlik duvarı tarafından korundukları yerlerde bile durumlarını görebileceğiniz anlamına gelir. –sN

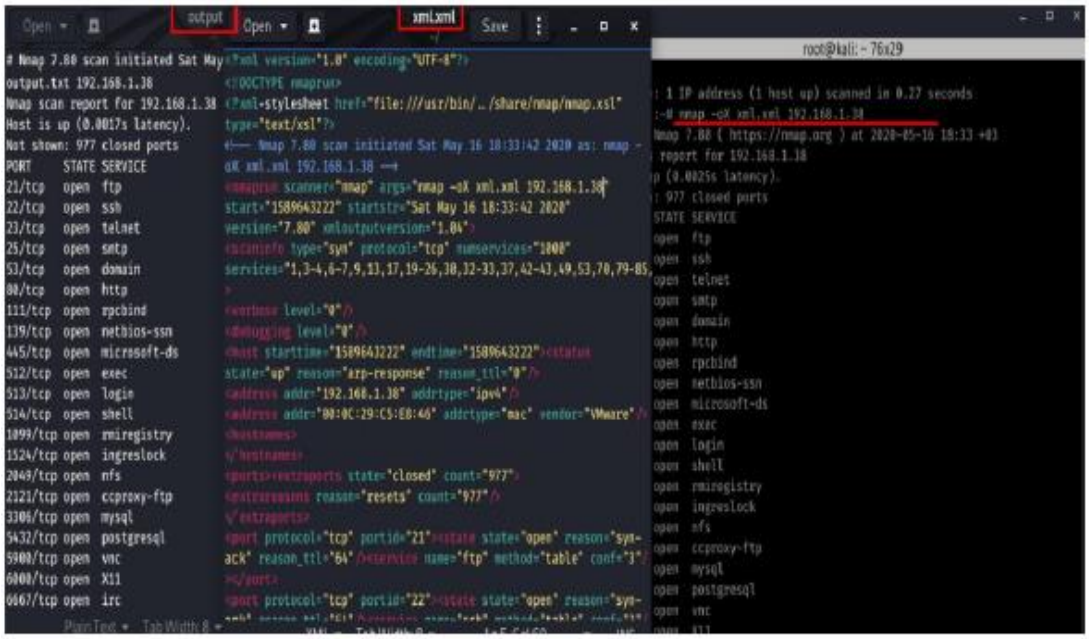
İlgili resimde, en çok kullandığımız ve çoğu kullanıcıya da ihtiyaç duyduğu tüm bilgileri veren, saniyede binlerce bağlantı noktasını tarayan ve bir TCP bağlantısını tamamlamadığın dan şüphe uyandırmayan –sS parametresi kullanıldı. nmap -sS 192.168.1.0/24 komutu ile ağımdaki bütün cihazların taramasını gerçekleştirildi. Örnekte de görüldüğü gibi ev ağımda buluna cihazlar listelenerek açık port ve servisler tespit edildi. Birden fazla portun açık olduğu görüntülenen 192.168.1.40 IP adresi, test için kurduğum metasploitable2 sistemimin IP adresidir. Sızma testi uzmanları veya saldırganlar bu çıktılar doğrultusunda ilgili blokta açık bulunan, tespit ettikleri port ve servisler üzerinden saldırılar gerçekleştirir. Tespit edilen servislerde zafiyetler bulunabilir ve bu zafiyetler ile sistem ele geçirilebilir veya bir sonraki adımlar için daha detaylı bir saldırı yol haritası çıkartılabilir.



Şekil 7.2 : Nmap

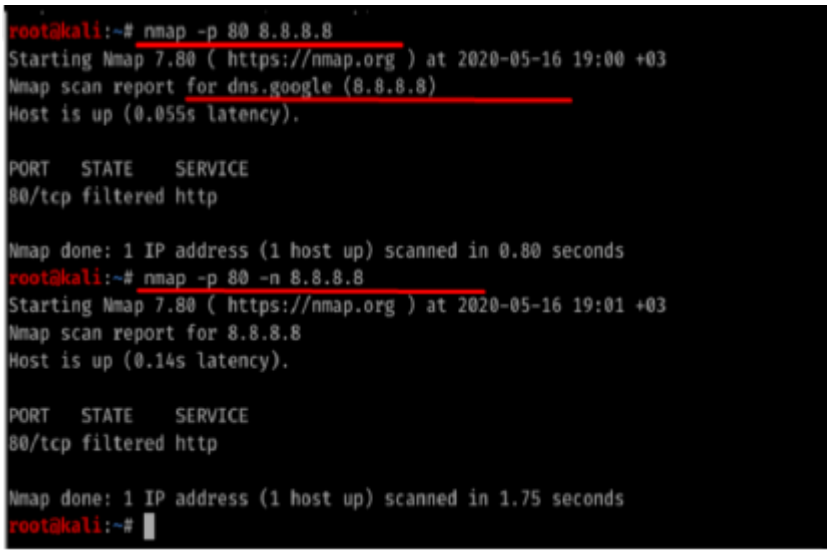
Yapılan taramaları çıktı almamız, daha sonra farklı araçlar ile saldırı yöntemleri geliştirmemize de yardımcı olacaktır. TXT ve XML çıktılarımızı metasploitable2

sistemimiz IP adresinde alacağız. XML için nmap -oX xml.xml 192.168.1.38 ve TXT çıktısı içinde nmap -oN output.txt 192.168.1.38 parametreleri kullanılmaktadır.



Şekil 7.3 : Nmap

Daha hızlı tarama yapabilmemiz için ters DNS çözümlemesini devre dışı bırakmayı seçebilirsiniz. Bunun için "-n" parametresini eklemeniz yeterli olacaktır. –n parametresi DNS çözümlemesi yapma anlamına gelmektedir. Sağdaki resimde kullanılan parametreler, «-p 80» sadece 80 portunu, –n parametresi ile DNS çözümlemesi yapmadan gerçekleştirmesi istenmektedir. nmap -p 80 -n 8.8.8.8

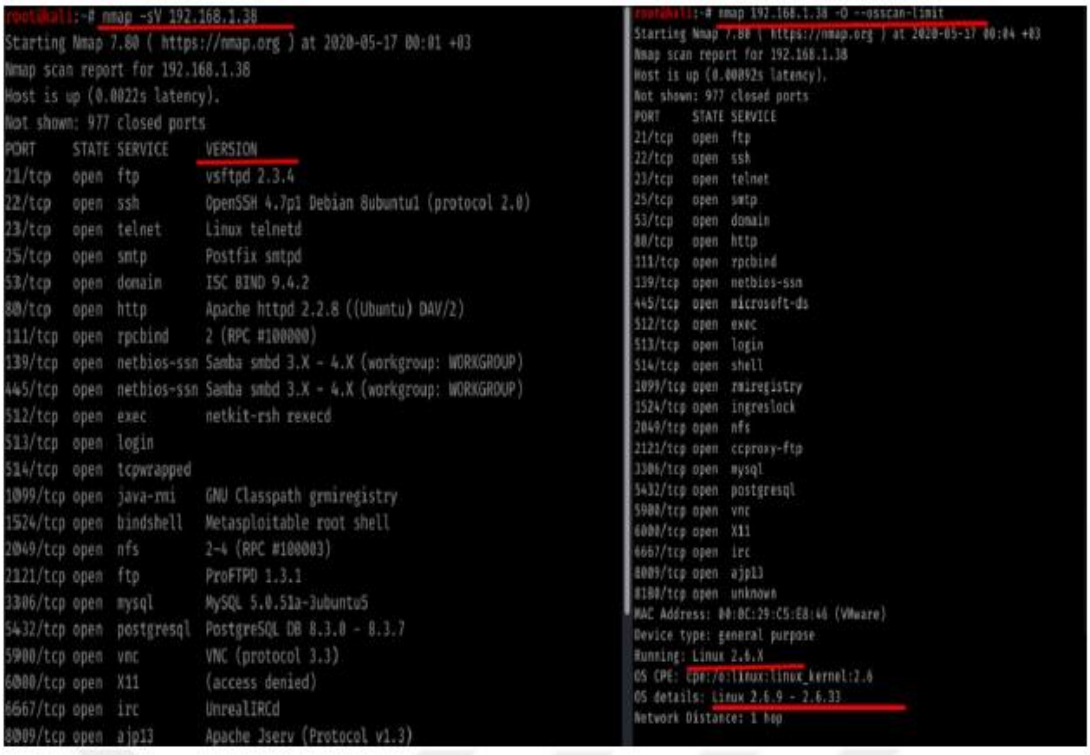


Şekil 7.4 Nmap

İşletim sistemi ve versiyon tespiti yapabilmemiz için –A parametresi kullanacağız. –A parametresi İşletim sistemi algılama, sürüm algılama, komut dosyası tarama ve traceroute'u etkinleştirir. Sağdaki resimlerde metasploitable sistemimize yaptığımız istek yer almaktadır. Burada altı çizilen yerlerde, tespit edilen servisler, tracerouter taraması ve işletim sistemi ile ilgili bilgiler ön plana çıkartılmıştır. Tespit edilen işletim sistemi ve servis versiyonları ile zafiyet araştırılması yapılarak, exploit çalışmaları gerçekleştirilir.

Hedef bağlantı noktasında çalışan hizmetlerin sürümünü belirlemek için nmap –sV 192.168.1.38 parametresi kullanılır. Sürüm tespit seviyesi 0 ile 9 arasındadır. -sV --version-all komutu, Yoğunluk seviyesi 9'u etkinleştirin ve daha yavaş bir tarama ile doğruluk olasılığı arttırır.

-O İşletim sistemi algılamayı etkinleştir. -O --osscan-limit parametresi TCP bağlantı noktası bulunursa işletim sistemi algılama çok daha etkilidir. Bu parametre kullanıldığında Nmap, ölçütleri karşılamayan ana bilgisayarlara karşı işletim sistemi algılamayı bile denemez. Bu, özellikle birçok ana bilgisayara karşı yapılan taramalarda önemli ölçüde zaman tasarrufu sağlayabilir.



Şekil 7.5 : Nmap

• Gönderilen ve alınan tüm paketleri göstermesi için --packet-trace komutu kullanılır. Tarama sonunda hedef makinede açık portları ve servisleri listeler.

• -v, -vv, -vvv komutları, ekrana gösterilecek detayları arttırır.

• Hızlı tarama gerçekleştirmek için –F parametresi kullanılır. Varsayılan taramadan daha az sayıda bağlantı noktası tarar.

• -T <0-5>: Zamanlama şablonunu ayarlar. Ve taradığı bloktaki bütün portları ve servisleri listeleyebilir.

• --open: Sadece açık Portları gösterir.

• nmap –P0 parametresi portlara ping atmadan açık olup olmadığını kontrol eder. ICMP kapalı sistemlerde bu parametre işe yarayabilir.

• TCP Connect Scan; nmap -sT ip_adres aynı şekilde portun açık olup olmadığını kontrol eder. Daha yavaştır ama güvenilirdir.

Şekil 7.6 : Nmap

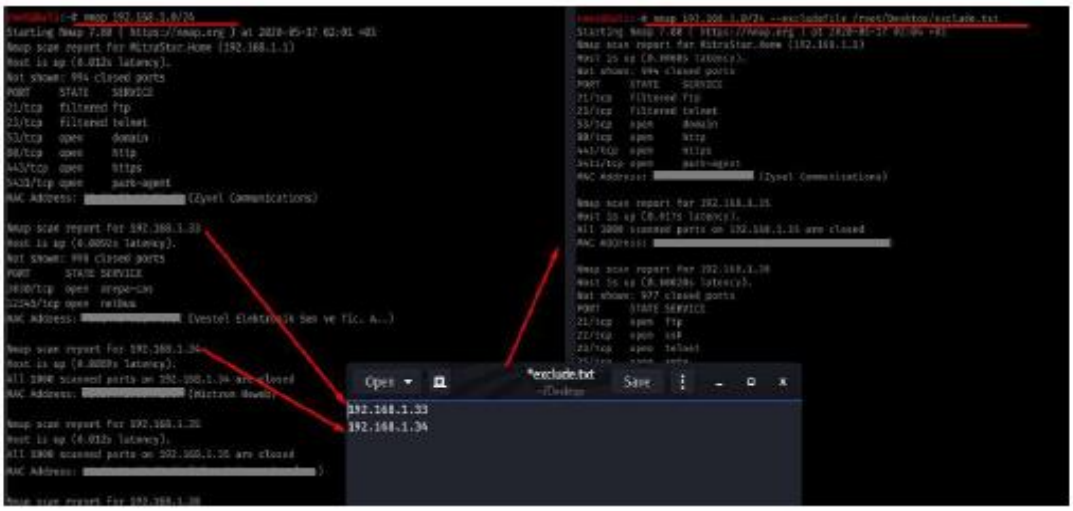
• --host-timeout <zaman> parametresi 1s; 4m; 2s süreleri belirlenerek, belirlenen süre içerisinde hedeften yanıt gelmez ise vazgeç anlamına gelmektedir.

• --min-rate <number> ve --max-rate <number> parametreleri, tarama hızlarını doğrudan kontrol eder. Hedef ağın tarama hızının ne kadar olacağını veya ne kadar sürede bitebileceğini biliyor veya tahmin ediyorsanız bu parametreler bu gibi durumlar için çok uygundur. Veya nmap taramaların hızlı bir şekilde gerçekleşmemesi için kullanabilirsiniz. Örneğin belirtmek --min-rate 300, Nmap'ın gönderme hızını saniyede 300 paket veya üstünde tutmaya çalışacağı anlamına gelir. Benzer şekilde, --max-rate taramanın gönderme hızını belirli bir maksimuma sınırlar. Örneğin --max-rate 100 hızlı bir ağda saniyede 100 paket gönderiyle sınırlamak için kullanılır.

• XMAS Scan «–sX» komutu diğer komutların açık port bulamadığı zaman devreye girer. Hedef sisteme bütün bayrakları içeren bir paket yollar, kapalı olan portların RST cevabı beklenir. Kapalı portlar cevap verdikten sonra cevap gelmeyen portlar açık olarak kabul edilir. nmap -sX ip_adres

• UDP taramaları gerçekleştirebilmek için «–sU» komutu kullanılır. Bu komut açık olan UDP portlarını tespit için kullanılır. nmap -sU ip_adres

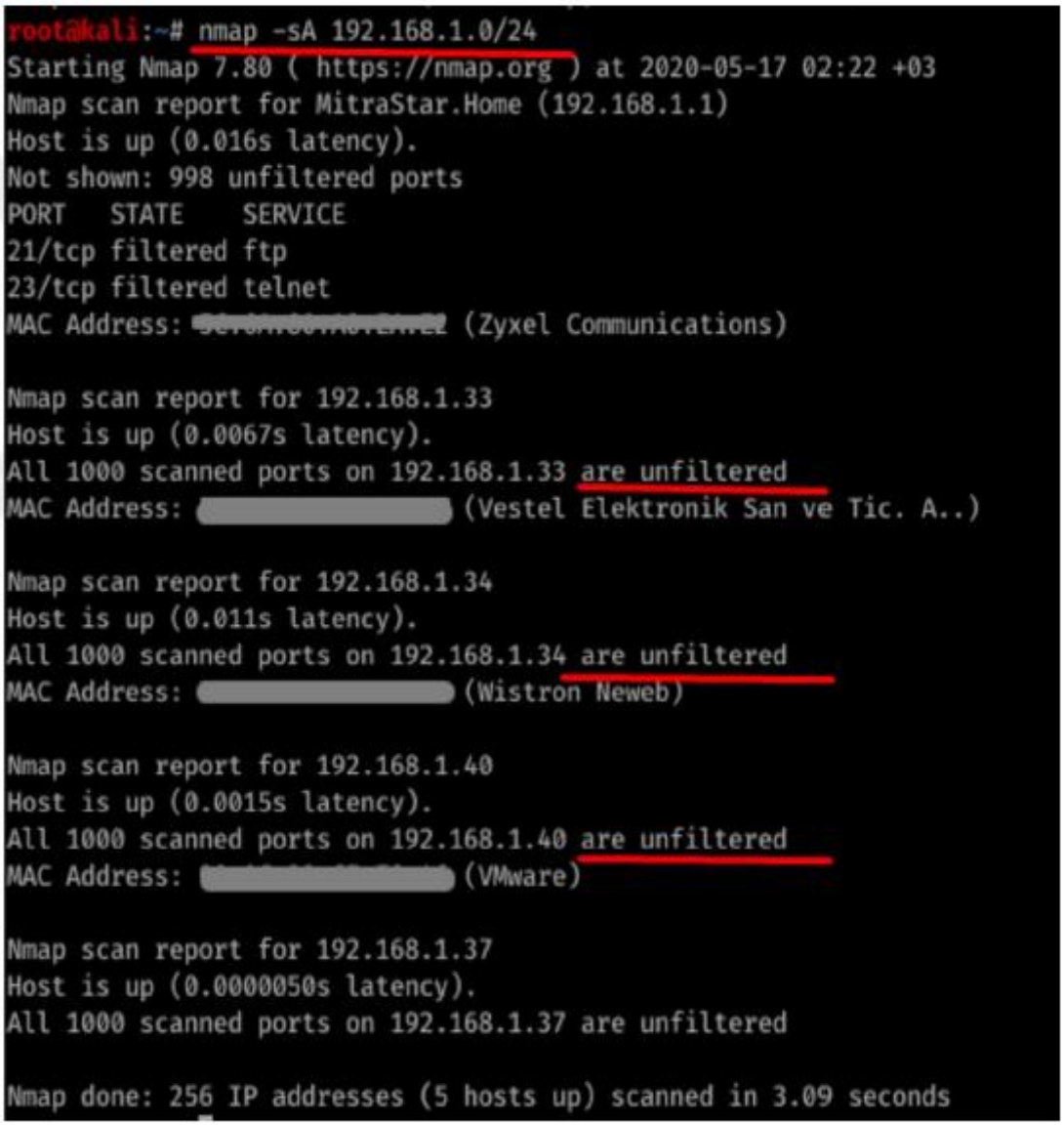
• Tarama yapılacak bir blokta, tarama yapılmaması istenilen IP adreslerini –excludefile parametresi ile hariç tutulur. nmap 192.168.1.0/24 –excludefile exclude.txt Aşağıdaki örnek tarama resminin bir kısmında, normal taradığımızda elde ettiğimiz IP adresleri ve bu adreslere bağlı bilgiler yer almaktadır. Diğer bir kısmında ise –excludefile komutu kullanarak, normal taramada elde ettiğimiz birkaç IP adresini bir TXT dosyasına ekleyerek, --excludefile komutu ile taramasını engellediğimiz sonuç yer almaktadır.



Şekil 7.7 : Nmap

• Nmap güvenlik duvarı TCP ACK taraması yapmak için, hedef bağlantı adresi ve –sA komutu ile Nmap çağrılmalıdır. Herhangi bir portun filtrelenip filtrelenmediğini belirlemeye çalışır. Bu teknik, herhangi bir ana bilgisayarı koruyan güvenlik duvarının durum bilgisini kontrol etmek için kullanışlıdır. nmap -sA «ip_adres» bu taramaya –p80 komutu ekleyerek, ilgili IP adresteki sadece istenilen portu taramasını isteyebilirsiniz. Veya başka komutlar ile taramanızın kapsamını genişletebilirsiniz.

• Firewall ile koruna bir hosts --PN parametresi ile taranabilir. Bu seçenek, Nmap keşif aşamasını tamamen atlar.



Şekil 7.8 : Nmap

7.3 Essential NetTools

Essential NetTools, ağları tanılamada ve bilgisayarınızın ağ bağlantılarını izlemede yararlı olan bir dizi ağ tarama, güvenlik ve yönetici aracıdır. Günlük kullanım için güçlü bir ağ araç kitiyle ilgilenen herkes için bir İsviçre Çakısıdır.

NetStat: açık TCP ve UDP bağlantı noktaları, IP adresi ve bağlantı durumları hakkındaki bilgiler de dahil olmak üzere bilgisayarınızın gelen ve giden ağ bağlantılarının bir listesini görüntüler. Onu diğer NetStat yardımcı programlarından farklı kılan şey, açık bağlantı noktalarını sahip olunan uygulamayla eşleme yeteneğidir. Gelen ve giden bağlantılar için yapılandırılabilir uyarılar da mevcuttur.

NBScan: güçlü ve hızlı bir NetBIOS tarayıcısı. NBScan, belirli bir IP adresi aralığındaki bir ağı tarayabilir ve NetBIOS kaynak paylaşım hizmeti sunan bilgisayarların yanı sıra ad tabloları ve MAC adreslerini listeleyebilir. Windows ile sağlanan standart nbtstat yardımcı programından farklı olarak, bu araç bir grafik kullanıcı arabirimi ve lmhosts dosyasının kolay yönetimini sağlar ve paralel tarama özelliğine sahiptir, bu da C sınıfı bir ağı bir dakikadan daha kısa sürede kontrol etmeye olanak tanır. NBScan, genellikle sistem entegratörleri, yöneticiler ve analistler tarafından gerçekleştirilen rutin görevleri kolaylaştırabilir.

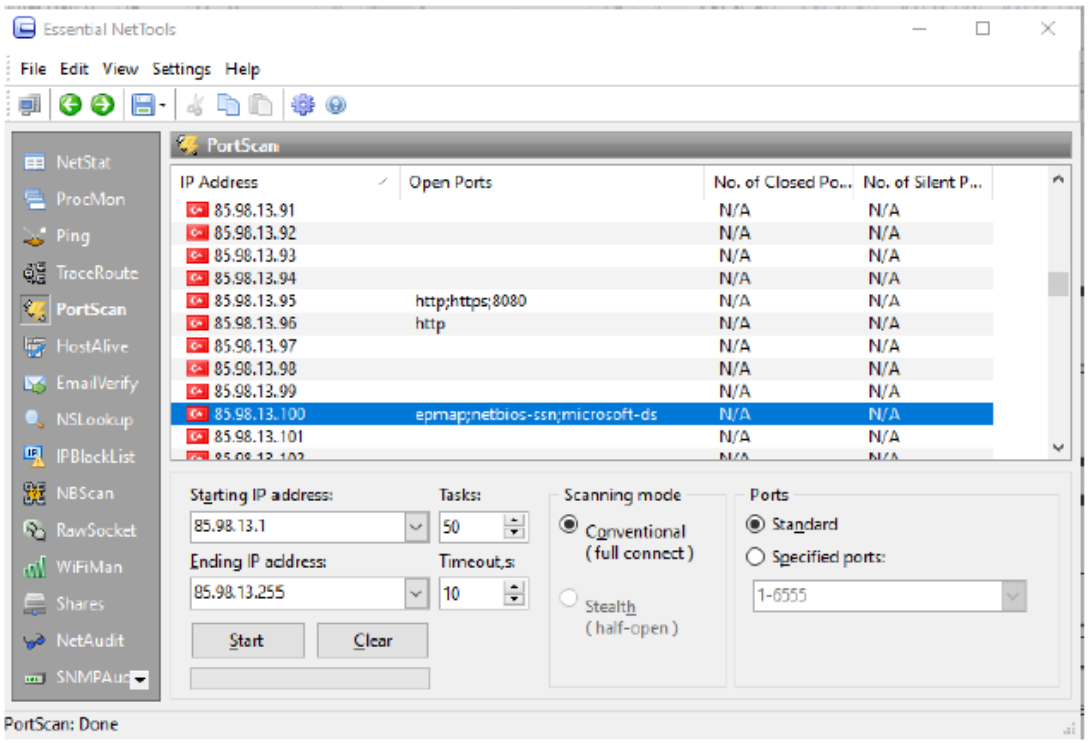
PortScan : ağınızı aktif portlar için taramanıza izin veren gelişmiş bir TCP port tarayıcı. Bu araç hem geleneksel (tam bağlantı) hem de gizli (yarı açık) tarama modlarına sahiptir.

HostAlive : bir ana bilgisayarın canlı olup olmadığını ve HTTP veya FTP sunucusu gibi ağ hizmetlerini çalıştırıp çalıştırmadığını düzenli olarak kontrol eden bir ağ izleme aracı.

EmailVerify : SMTP üzerinden ilgili posta sunucusuyla iletişim kurarak bir e-posta adresinin geçerli olup olmadığını kontrol eder.

Paylaşımlar : Bilgisayarınızın paylaşılan kaynaklarına yapılan harici bağlantıları izler ve günlüğe kaydeder, yerel paylaşımları listeler ve ayrıca uzak kaynaklara bağlanmak için hızlı ve kolay bir yol sağlar.

SysFiles : beş önemli sistem dosyası için uygun bir düzenleyici: hizmetler, protokol, ağlar, ana bilgisayarlar ve lmhost'lar



Şekil 7.9: Essential NetTools

NetAudit (NetBIOS Denetim Aracı): ağınızda ve/veya NetBIOS dosya paylaşım hizmeti sunan bireysel bilgisayarlarda çeşitli güvenlik kontrolleri yapmanızı sağlar. Bu araç, olası güvenlik açıklarını belirlemenize yardımcı olabilir.

RawSocket: farklı ağ hizmetlerinde sorun gidermek ve test etmek için size düşük seviyeli TCP ve UDP bağlantıları kurma yeteneği sağlar. Çok renkli çıktı ve kullanışlı bir arayüz, onu her ağ yöneticisi veya bilgisayar programcısı için harika bir araç haline getirir.

WiFiMan: bir bilgisayarda kurulu kablosuz bağdaştırıcıları gösterir, kullanılabilir kablosuz ağları listeler ve bağlantı profillerini yönetmenize olanak tanır.

TraceRoute ve Ping: Özelleştirilebilir seçenekler ve kullanışlı sonuç sunumu içeren bu tanıdık yardımcı programlar, İnternet'i keşfetmenize ve bağlantı sorunlarını gidermenize olanak tanır.

NSLookup: IP adreslerini ana bilgisayar adlarına veya tam tersine dönüştürmenize, takma adlar almanıza ve MX veya CNAME gibi gelişmiş DNS sorguları gerçekleştirmenize olanak tanır.

IPBlackList: bir IP adresinin farklı IP adresi kara listelerinde olup olmadığını kontrol eder: SPAM veri tabanları, açık proxy'ler ve posta geçişleri, vb. Bu araç, belirli bir IP adresinin posta sunucuları gibi bazı ağ kaynakları tarafından neden reddedildiğini anlamamıza yardımcı olur.

ProcMon: Programın konumu, üretici ve işlem kimliği ile yüklenen modüller hakkında tam bilgilerle birlikte çalışan işlemlerin listesini görüntüler. Bu araçla, CPU kullanım istatistiklerini görüntüleyebilir, gizli uygulamaları belirleyebilir, çalışan işlemleri sonlandırabilir ve bilgisayarınızın kaynaklarının kullanımını daha etkin bir şekilde yönetebilirsiniz.

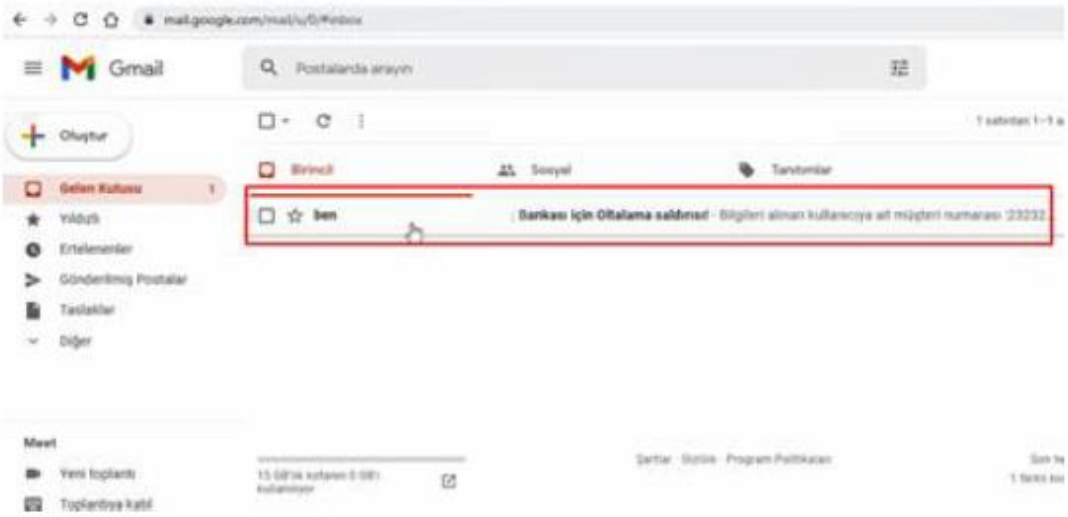
SNMPaudit: Gelişmiş SNMP cihaz tarayıcısı. Seçilen ağ segmentindeki SNMP cihazlarını hızlı bir şekilde bulmanıza ve her bir cihazdan özelleştirilebilir veri örneklemesi almanıza olanak tanır. Bir cihazı detaylı olarak incelemek için SNMP tarayıcısını kullanabilirsiniz. Diğer özellikler arasında HTML, metin ve virgülle ayrılmış biçimlerde rapor oluşturma; farklı araçlar arasında hızlı IP adresi paylaşımı; IP adresi coğrafi konumu kapsamlı bir Sistem Özeti penceresi ve özelleştirilebilir bir arayüz bulunmaktadır.

7.4 Phishing Saldırı Uygulaması

Siber saldırılarda en zayıf halka olan insan faktörü olduğunun kanıtlanması için yapılan phishing saldırı uygulaması yapılmıştır. Burada bir bankanın web sayfası kopyalanmış ve kurbana cazip bir kredi teklifi ya da güvenlik ihlali e-postası ile yollanan linke tıklaması sağlanmaya çalışılmıştır.

Şekil 7.10: Sahte Banka Web Sitesi Ekranı

Kopyalanan bir banka sitesi kodları değiştirilerek kurbanın bilgilerini girmesi sağlanmaktadır. Girilen bilgiler ilgili değişikliklerle belirlediğimiz bir mail adresine gelmesi sağlanmaktadır. Böylelikle ele geçirilmek istenilen bilgilere erişim imkanı sağlanmaktadır.



Şekil 7.11: Mail Adresi Ekranı

Sahte web sayfasının yönlendirmesi ile mail adresine gelen bilgiler mail kutusunda gözükmektedir. Bu bilgiler hızla bankanın web sitesine girilerek ilgili siber saldırı gerçekleştirilir.

8. SONUÇ VE ÖNERİLER

Kali Linux NMAP aracı ile genel keşif ve bilgi toplama işlemi yapılmıştır. Yapılan bu taramada zafiyet amaçlı açık port olup olmadığına bakılmıştır. Tarama sonrası, saldırı amaçlı açık bir port olmadığı gözlenmiştir. Genelde açık olan 80 portu'nun (HTTP listening port) web sayfası amaçlı kullanıldığı bilinmektedir.

Alınan tedbirlerin yanında kamu kurumları ve özel sektörün kullandığı sunucular ile kullandıkları uygulamaların uyumluluğu önem arz etmektedir. Birçok saldırgan uygulamaların kullandığı sunucuların güncel olmamasından kaynaklı açıklardan yararlanmaktadır. Bu nedenle sunucuların güncellemeleri tam ve eksiksiz olmalıdır. Kullanılan uygulamaların zamanımızın teknolojisine uygun yazılımlarına entegre olacak şekilde yenilenmesi ve tasarlanması gerekmektedir. Güncel olmayan sunucu her zaman tehlike arz etmektedir. Genellikle siber saldırılara maruz kalan sistemler açıkları kapatılmamış sunuculardan kaynaklanmaktadır. Tüm sistemin etkin bir anti virüs yazılımı ile korunması gerekmektedir. Bu korunma yerel bilgisayarlar ve taşra teşkilatı bulunan tüm kurumlar için muhakkak uygulanması gerekmektedir. E-posta hesapları için kullanılan şifre, diğer hesaplarınızdaki şifrelerden farklı yapıda olmalıdır. Kullanılan bu şifreler sosyal medyalar ya da alışveriş sitelerinde kullanılan şifreler olmamalıdır.

Kişisel bilgileri isteyen e-postalara yanıt verilmemelidir. Gelen e-postanın kimden geldiği bilinmiyorsa dikkate alınmamalıdır. Unutulmamalıdır ki hiçbir kurum veya kuruluş, çalıştığınız işyeri bile asla kişisel verilerinizi ve parolanızı soran e-posta göndermez. Şüpheli görülen e-postalardaki URL linkleri tıklanmamalıdır. E-posta mesajlarındaki kısaltılmış URL linklerine (bit.ly, ow.ly, tinyurl.com, is.gd, goo.gl, tiny.cc, cli.gs vb.) herhangi bir internet tarayıcı ile açılması tehlikeli hale gelebilmektedir. Şüpheli veya bilinmeyen web sitelerine kişisel bilgiler ve kredi kartı bilgileri verilmemelidir. Bankaların kredi kartı ve servis sağlayıcılarının web siteleri ziyaret edildiğinde, kişisel bilgileri girmek için web sitesinin URL'si internet

tarayıcısına doğrudan yazılmalıdır. Güvenli olarak görülen sitelerde çevrimiçi olarak bir form doldurmadan, ilgili sitenin üçüncü kişilerle kişisel bilgileri paylaşıp paylaşmadığını belirten gizlilik anlaşmasının var olup olmadığının kontrolü sağlanmalıdır. Yasal olmayan veya kaynağı belirsiz yazılımlar yüklenmemeli ve çalıştırılmamalıdır. Ücretli olarak satılan ticari programları kullanmak için crackleri gelişi güzel çalıştırılmamalıdır. Kredi kartlarının numaraları, özel veriler dâhil her türlü parola asla e-posta ile açıkça iletilmemelidir. Bir e-posta teknik anlamda gideceği yere ulaşana kadar birçok yerden geçmektedir. Bu yerlerden geçerken e-postaların içeriğinin "dinlenmesi" mümkün olabilir. Halka açık kablosuz erişim ağının kullanıldığı yerlerde mecbur olmadıkça bankaların web sitelerine girilmemeli, kart bilgileri, parola vs. ile ilgili hiçbir şey yapılmamalıdır. Sinyaller üçüncü şahıslar tarafından dinlenebilir. Bu sinyaller şifreli bile olsa unutulmamalıdır ki tüm şifreleme yöntemleri sadece kırılıncaya kadar güvenlidir. Bankalardaki hesapların güvenliğini sağlamak ve bu tip saldırıları önlemek için Kare kod tarama uygulaması ya da cep telefonunuzdaki banka uygulamasına giriş yapıldığında doğrulama onayı vererek giriş yapmak bu tip tehditlerin önüne geçecektir. Kendini savcı, polis, asker olarak tanıtan kişiler “kumpas kuruldu hakkınızda dosyalar var” gibi ifadelerle para istemektedir. Hiçbir savcı, polis veya asker telefon yolu ile sizden para istemez.

Siber zafiyetlerin giderilmesinde insan faktörü ve insanların eğitimi çok önemlidir. Bu farkındalık eğitimlerinin artırılması için Cumhurbaşkanlığı Dijital Dönüşüm Ofisi öncülüğünde BTK ile birlikte tüm kamu kurum ve kuruluşlarında çalışmalar yürütülmektedir. Ayrıca 27001 Bilgi güvenliği kapsamında BGYS (Bilgi Güvenliği Yönetim Sistemi) kamu kurumlarında denetimler yapılmaktadır. En önemli gelişme Siber güvenlik eğitimlerinin ilkokul çağından itibaren başlanarak verilmesi amacıyla Milli Eğitim Bakanlığının bünyesindeki EBA sisteminde “Siber Güvenlik Portalı” oluşturulmuştur. Bu portal öğretmenlere, ailelere ve öğrencilere yol gösterecek bir rehber niteliğinde olacaktır. Tüm bu değerlendirmelere göre siber saldırılara karşı alınacak tedbirler kişisel olsa da “Saldırı Tespit ve Önleme Sistemleri’nin” varlığı çoğu kuruluşun güvenlik zafiyetlerini azaltmıştır. Yapılan saldırılar ve bunların çeşitliliği göz önüne alındığında her saldırı tipine ve çeşidine göre cihaz almanın da bir maliyeti olmaktadır. Ancak hiçbir maliyet veri güvenliğinden daha önemli değildir. Yaptığım incelemelerde kamu kurumlarında alınan güvenlik tedbirleri ile Siber

Güvenlik personelinin varlığı, son dönemde yapılan siber saldırılarda çok etkili ve etkin olmuştur.

Kaynaklar

[1] Ada, M. (2018). NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi. Gazi Üniversitesi Bilişim Enstitüsü, Yüksek Lisans Tezi, Ankara.

[2] Akdeniz, H. (2020). Değişen Güvenlik Konsepti Ve Güvenliğin Yeniden Kavramsallaştırılması, Change in State Nature: Boundaries of Security, s.63- 80.

[3] Şentürk M.Y., Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinde Uygulanması, Yüksek Lisans Tezi, Türk Hava Kurumu Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2018, 527395.

[4] Çakır, S., Kesler, M. (2012). Bilgisayar güvenliğini tehdit eden virüsler ve antivirüs yazılımları. XIV. Akademik Bilişim Konferansı Bildirileri, 551-558.

[5] İren, E., & Can, Ö. (2017). Bilgi Sistemlerinde Güncel Güvenlik Problemleri Ve Önerilen Çözümler. TÜBAV Bilim Dergisi, 33.

[6] Güntay, V. (2018). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi Ve Uluslararası Aktörler. Güvenlik Stratejileri Dergisi, 100- 101.

[7] Abdulkareem, M. (2012). IEEE 802.11 Kablosuz Ağlarda Güvenlik (Yüksek Lisans Tezi). Ankara.

[8] Tombul, H. (2019). Siber Savaşlar Ve Siber Silahlar. Siber Savunma Ve Güvenlik Problemler Ve Çözümler (S. 382-384). İçinde Ankara: Grafiker Yayınları.

[9] Sağıroğlu, A. (2018). Siber Güvenlik Ve Savunma: Önem, Tanımlar,Unsurlar Ve Önlemler. A. M. Sağıroğlu Şeref Ve İçinde, Siber Güvenlik Ve Savunma (S. 25). Ankara: Grafiker Yayınları.

[10] Özkaya Vd., S. ,. (2019). Bilişim Sistemlerine Yönelik Tehditler. R. S. Erdal Özkaya İçinde, Siber Güvenlik Saldırı & Savunma Stratejileri (S. 45). Ankara: Buzdağı Yayınevi.

[11] Özkaya Vd., S. ,. (2019). Ağ Güvenliği. E. Özkaya, R. Sarıca, & Ş. Durmaz İçinde, Siber Güvenlik Saldırı & Savunma Stratejileri (S. 343 - 344). Ankara: Buzdağı Yayınları.

[12] Aslan, Ö., & Samet, R. (2018). Kötü Amaçlı Yazılımlar Ve Analizi. Siber Güvenlik Ve Savunma Farkındalık Ve Caydırıcılık (S. 227). İçinde Ankara: Grafiker Yayınları.

[13] San, İ. (2016). Sistem Güvenliği. E. A. Bilge İçinde, Ağ Yönetimi Ve Bilgi Güvenliği (S. 159-160). Eskişehir: Anadolu Üniversitesi Yayınları.

[14] İstanbul Üniversitesi Kariyer GeliĢtirme Uygulama ve AraĢtırma Merkezi. (2015). Siber Saldırı Türleri. Bilişim'de Kariyer(2), 12-13.

[15] Akyıldız M.A., Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ile Değerlendirilmesi, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, Isparta, 2013, 353566.

[16] Uçan O.N., Osman O., Bilgisayar Ağları ve Ağ Güvenliği, 1.Baskı, Nobel, Ankara, 2006

Özgeçmiş

Adı Soyadı: Fethi ÇOBAN
E-mail (1): fethicoban@ikcu.edu.tr
E-mail (2): fethicobann@gmail.com

Eğitim:

2011–2012 Piri Reis Üniversitesi, Deniz Ulaştırma ve İşletme Müh. Bölümü
2013–2014 Fırat Üniversitesi, Mekatronik Müh. Bölümü
2014-2017 İstanbul Gelişim Üniversitesi, Mekatronik Müh. Bölümü
2017-2018 Hava Teknik Okullar Komutanlığı, MEBS Subaylığı

İş Deneyimi:

2017–2017 Mondelez İnternational, Bakım Mühendisi
2018- Hava Kuvvetleri K.lığı 2'nci Ana Jet Üs K.lığı, Muhabere Elektronik Sistemler Bölük Komutanı