Araştırma Makalesi

AĞ ORTAMINDAKİ SALDIRI TÜRLERİ: SALDIRI SENARYO ÖRNEKLERİ

Fırat KILINÇ[†], Can EYÜPOĞLU[††]

[†] Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul, Türkiye

[††] Milli Savunma Üniversitesi, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye

firatkilinc35@gmail.com, caneyupoglu@gmail.com

0009-0001-5611-7908, 0000-0002-6133-8617

Atıf/Citation: KILINÇ, F., EYÜPOĞLU, C., (2023). Ağ Ortamındaki Saldırı Türleri: Saldırı Senaryo Örnekleri, Journal of Technology and Applied Sciences 6-1 pp99-109 DOI: 10.56809/icujtas.1282687

ÖZET

Çağımızda bilgi teknolojileri hızla gelişirken mobil ve nesnelerin interneti (Internet of Things-IoT) cihazlarının yaygınlaşması ile birlikte siber saldırganlar da her geçen gün yeni saldırı yöntemleri geliştirmektedir. Bu nedenle siber saldırılar kullanıcılarda büyük endişe yaratmakta ve bu endişelerin de giderek artacağı öngörülmektedir. Bu süreçte Saldırı Tespit Sistemleri (Intrusion Detection System-IDS) ve Saldırı Önleme Sistemleri (Intrusion Prevention System-IPS) önemli bir rol almaktadır. Bu çalışmada ilk olarak ağ güvenlik duvarları, ağ saldırıları ve ağ ortamında gerçekleşen saldırı türlerine yer verilmiştir. Sonrasında ağ saldırı türleri için örnek senaryolar oluşturulmuş ve bu senaryolar üzerinde saldırıların nasıl gerçekleştirildiği açıklanmıştır. Saldırı türleri, Kanada İletişim Güvenliği Kuruluşu (Canada Communications Security Establishment-CSE) ve Kanada Siber Güvenlik Enstitüsü (Canadian Institute for Cybersecurity-CIC) tarafından yaratılan saldırı tespit sistemi değerlendirme veri setlerinde (CIC-IDS2017 ve CES-CIC-IDS2018) yer alan ve saldırganlar tarafından yaygın olarak kullanılan hizmet reddi saldırısı (Denial of Service Attack-DoS), dağıtık hizmet reddi saldırısı (Distrubuted Denial of Service-DDoS), botnet, kaba kuvvet, port tarama, web uygulama ve sızma saldırıları olarak belirlenmiştir.

Anahtar Kelimeler: Siber Saldırı Türleri, Saldırı Tespit Sistemi, Saldırı Önleme Sistemi, CIC-IDS2017, CES-CIC-IDS2018

ATTACK TYPES IN NETWORK ENVIRONMENT: ATTACK SCENARIO EXAMPLES

ABSTRACT

While information technologies are developing rapidly in our age, with the spread of mobile and Internet of Things (IoT) devices, cyber attackers are developing new attack methods day by day. For this reason, cyber attacks cause great concern for users and it is predicted that these concerns will increase gradually. In this process, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play an important role. In this study, firstly, network firewalls, network attacks and attack types in network environment are mentioned. Afterwards, sample scenarios for network attack types are created and how the attacks are carried out on these scenarios are explained. The attack types are determined as Denial of Service Attack (DoS), Distributed Denial of Service (DDoS), botnet, brute force, port scan, web application and infiltration, which are included in intrusion detection evaluation datasets (CIC-IDS2017 and CES-CIC-IDS2018) created by Canada Communications Security Establishment (CSE) and Canadian Institute for Cybersecurity (CIC), and are widely used by attackers.

Keywords: Cyber Attack Types, Intrusion Detection System, Intrusion Prevention System, CIC-IDS2017, CES-CIC-IDS2018

Geliş/Received	:	**13.04.2023**
Gözden Geçirme/Revised	:	**16.05.2023**
Kabul/Accepted	:	**07.06.2023**

1. GİRİŞ

Son yıllarda, siber saldırıların sayısında ve çeşitliliğinde önemli bir artış görülmektedir. Ev kullanıcıları, kurumsal işletmeler, devlet kurumları ve kritik altyapılar siber saldırganlar tarafından hedef alınmaktadır. Birçok durumda, ağlara ciddi zararlar vermeden önce saldırıları çok erken aşamalarda tespit etmek önemlidir. Bu amaçla, siber güvenlik araştırmacıları ve profesyonelleri tarafından gerçek zamanlı savunma araçlarından olan saldırı tespit sistemleri (Intrusion Detection System-IDS) ve saldırı önleme sistemleri (Intrusion Prevention System-IPS) geliştirilmektedir.

Günümüzde siber güvenlik, toplumda önemli bir endişe kaynağı olmuştur. Devlet kurumları ve kurumsal işletmeler hakkındaki bilgiler hayati derecede önemli olmasından dolayı güvenli bir şekilde muhafaza edilmelidir. Bu bilgiler, yetkisiz veya üçüncü kişilerin erişemeyeceği bir yerde saklanmalıdır.

Güvenli bilgileri muhafaza etmek zor olabilir ve her zaman saldırganlar tarafından bir güvenlik ihlali riski olasılığı vardır. Genellikle en yaygın tehditler; bir web sitesine karşı düşmanlık, siber yarışmalar, fidye, siyasi mesele, eğlence vb. nedenlerle web sunucularının çökertilmesine yönelik yapılan saldırılardır. Siber güvenliğinin temelini oluşturan gizlilik, bütünlük ve erişilebilirlik üçlüsü güvenlik sistemlerinde etkin bir şekilde uygulanmalıdır (James, 2019).

Bu çalışmada CIC-IDS2017 ve CES-CIC-IDS2018 veri setlerinde ağ güvenliği ve izinsiz giriş tespit amaçları için kullanılan saldırı senaryolarına yer verilmiştir. Çalışmanın diğer bölümleri şu şekilde düzenlenmiştir: Bölüm 2'de saldırı tespit sistemleri, saldırı önleme sistemleri ve bu ikisi arasındaki farklar ele alınmıştır. Bölüm 3'te saldırganların amaçları ile kötü amaçlı yazılımların belirtileri incelenmiştir. Bölüm 4'te ağ ortamında gerçekleşen saldırı türleri (hizmet reddi saldırısı, dağıtık hizmet reddi saldırısı, botnet saldırısı, kaba kuvvet saldırısı, port tarama saldırısı, web uygulama saldırısı ve sızma saldırısı) hakkında detaylı bir inceleme yapılarak örnek senaryolar ile anlatılmıştır. Bölüm 5'te ise çalışmanın genel sonuçlarından bahsedilmiştir.

2. AĞ GÜVENLİK DUVARLARI

İnternet ağındaki veriler istemci bilgisayar kullanıcısına gönderilen ve hangi kaynaktan gelip, hangi hedefe ulaşması gerektiğine ilişkin bilgileri içermektedir. Ağ güvenlik duvarları ise istemci bilgisayar kullanıcılarını internet ağındaki kötü huylu saldırgan veri trafiklerinden savunan donanım ve yazılım araçları olarak tanımlanabilirler. Ağ yöneticisi tarafından ağ güvenlik cihazı üzerinde veri akış trafiğini denetlemek için kurallar tanımlanır. Ağ yöneticisi tarafından tanımlanmış olan kurallar yetkisiz kişilerin ve istenmeyen verilerin yerel ağlara girmesini engeller; bu sayede ağlar arasındaki güvenli veri trafiği düzenlenir ve ağ cihazları kötü amaçlı saldırılara karşı korunmuş olur. Bu kurallar dizisinde zararsız olduğu tanımlanan verilerin geçişine müsaade edilirken zararlı veri olduğu tespit edilenlerin ağ dışında kalması sağlanır. Ağ üzerindeki saldırıları tespit etmek ve önlemek için kullanılan sistemler literatürde temel olarak IDS ve IPS olmak üzere iki ana başlıkta incelenir.

2.1. Saldırı Tespit Sistemleri

IDS'ler özel bir ağ aygıtı veya bir sunucu üzerine kurulabilen güvenlik duvarlarındaki kötü amaçlı trafikleri tespit etmek için kullanılır. Temelde bu trafiklerin kötü amaçlı olup olmadığı, kural tabanlı ve imza tabanlı olmak üzere iki farklı analiz yöntemi ile gerçekleştirilir (Taner, 2019). IDS tarafından söz konusu kötü amaçlı trafikler günlük olarak tespit edilir, yapılan tespitler sisteme kaydedilir ve ağ yönetisine uyarı mesajı gönderilir. Özellikle, IDS tarafından kötü amaçlı trafiklere reaksiyon gösterilmez ve önlem alınmaz. Dolayısıyla, IDS'nin temel görevi saldırıları önlemek değil saldırıları tespit edip kaydetmek ve ağ yöneticisine raporlamak olarak ifade edilir.

IDS'nin en önemli dezavantajlarından birisi gerçekleştirdiği taramalar nedeniyle ağı yavaşlatmasıdır. Genellikle gecikme süresi olarak da ifade edilen bu yavaşlamayı engelemek amacı ile IDS'nin çevrim dışı çalıştırıldığı durumlar da söz konusudur (Taner, 2019). Bu yöntemde, sistemden geçiş yapacak veriler kopyalanarak ağ yöneticisi tarafından belirlenmiş kurallar kapsamında değerlendirilmesi maksadıyla çevrimdışı çalışan IDS'ye iletilir. Bunların dışında sunucu bilgisayarındaki işletim sisteminin (Linux ve Windows vb.) üzerine yüklenebilecek bir uygulama olarak da kullanılan IDS'ler mevcuttur.

2.2. Saldırı Önleme Sistemleri

IPS'de IDS'de ifade edilen görevlere ilave olarak ağ güvenliğini sağlayacak aktif çözümler bulunmaktadır (Taner, 2019). IPS, aynı IDS'de olduğu gibi ağ yöneticisince belirlenen kurallar ışığında veri trafiğini analiz ederek kötü amaçlı trafikler tespit eder. Ancak, ilaveten kötü amaçlı trafiklerin sistemlere girişinin engellenmesi de sağlanır. Tüm bunların yanında IPS'nin yaptığı işlemler sisteme kaydedilerek ağ yöneticisine raporlanır ve bu sayede daha efektif performans analizi yapılmasına imkan sağlanmış olur.

3. BİLGİSAYAR AĞ SALDIRISI

Bilgisayar ağ saldırısı, yerel ağdaki bir veya daha fazla istemci bilgisayar, sunucu veya ağ cihazlarını kullanım dışı bırakmak maksadıyla yapılmaktadır. Bu saldırılarda ağ yöneticisinin veya kullanıcının izni olmadan cihazlara erişim sağlamak, cihazlarda kullanılan uygulamaları bozmak ya da kullanım dışı bırakmak amacıyla bilinçli olarak yapılır.

Kötü niyetli kişiler veya siber suçlular tarafından gerçekleştirilen bu saldırılar, yerel ağ güvenliğinin açıklarını kullanan virüsler, zararlı ve casus yazılımlar ile yapılır. Özellikle, bu tür saldırılar ile ağ cihazları devre dışı bırakılarak kurumsal işletmeler veri hırsızlığı gibi maddi ve manevi büyük zararlara uğratılabilir.

3.1. Saldırganların Amaçları

Uluslararası Cisco Ağ Akademisi tarafından bilgisayar ağ saldırılarının hangi amaçla yapıldığı aşağıda sunulmuştur (Cisco Ağ Akademisi, 2023):

- Bilgi hırsızlığı: Genellikle kötü amaçlı bir yazılım, oltalama (phishing) (Gupta ve ark., 2016) ve kaba kuvvet (brute-force) (Tams ve ark., 2015) gibi yöntemlerle bir yerel ağa veya bir istemci kullanıcıya erişim sağlayarak verilerini ele geçirmek olarak tanımlanmaktadır.
- Veri kaybı: Genellikle kullanıcıların izni olmadan bir virüs aracılığı ile yerel ağda bulunan bilgisayar sabit diskindeki verileri değiştirmek veya yok etmek olarak açıklanmaktadır. Bu önemli verilerin kayıplarının yanı sıra finansal kayıplara, kurumların itibar eksikliklerine ve hukuki sorunlara sebep olabilmektedir.
- Kimlik hırsızlığı: Genellikle kişisel bilgilerin ele geçirilmesi olarak tanımlanmaktadır. Bu bilgiler şahısların kendisine ait kimlik bilgileri, kredi kartı bilgileri ve çevrimiçi işlemlerde kullanılan parola işlemleri ile ilgili değerli verilerin ele geçirilmesi olarak bilinmektedir. Saldırgan bu bilgilerle saldırıya uğrayan kişi veya kurumları birçok süreçte (bankacılık işlemleri ve yasal işlemler vb.) maddi ve manevi zararlara uğratabilmektedir.
- Hizmet kesintisi: Genellikle yerel ağda bulunan istemci bilgisayarın ağ sisteminden, sunuculardan veya ilgili web sayfalarından hizmet almalarını devre dışı bırakarak sistemin çalışmasını engellemek olarak tanımlanmaktadır. Son zamanlarda devletler tarafından sunulan çevrim içi hizmetler ve bankacılık işlemleri kurumsal şirketler için ciddi tehditler içermektedir. Bunlar hizmet reddi saldırısı (Denial of Service Attack-DoS) (Sharafaldin ve ark., 2018) veya dağıtık hizmet reddi saldırısıdır (Distrubuted Denial of Service-DDoS) (Akgun ve ark., 2022).

3.2. Kötü Amaçlı Yazılımların Belirtileri

Bilgisayar virüsü, solucan, truva atı, fidye virüsü, casus yazılım olarak bilinen kötü amaçlı yazılımların belirtileri aşağıdaki gibidir (Taner, 2019):

- Bilgisayarın işlemci kullanımında hızlı bir yükselme ve performansında bir yavaşlama olması,
- Bilgisayar sürücüsündeki verilerin değiştirilmiş veya yok edilmiş olması,
- Bilgisayarın web tarayıcısındaki başlangıç sayfası ve tarayıcı ayarlarının değiştirilmiş olması ya da bilinmeyen araç çubuklarının eklenmesi,
- Antivirüs programlarına erişilememesi ya da devre dışı bırakılması,
- Bilgisayarda bulunan kullanıcı hesaplarının veya e-posta hesaplarının çalınmış olması ve bu hesaplardan spam e-postalar gönderilmesidir.

4. AĞ ORTAMINDA GERÇEKLEŞEN SALDIRI TÜRLERİ

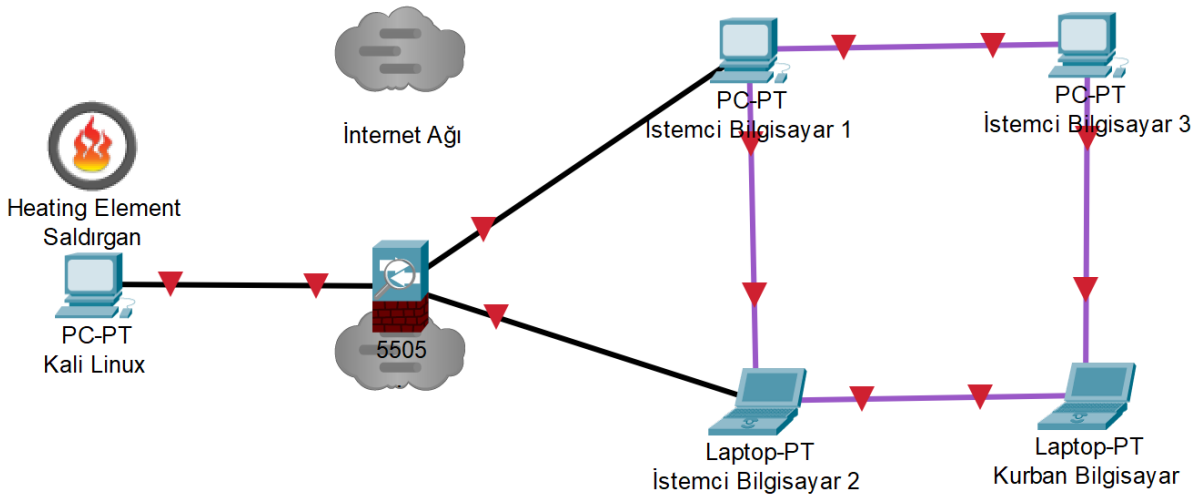
4.1. Hizmet Reddi Saldırısı

DoS saldırısı, bir saldırganın masum bir son kullanıcının bilgisayarını ve yerel ağ kaynağını kullanamamasına sebep olması olarak tanımlanmaktadır (Sharafaldin ve ark., 2018). DoS saldırıları uygulamada iki ana başlık altında incelenmektedir:

- Yoğun trafik miktarı: Saldırgan tarafından bir ağa, sunucu bilgisayarlarına veya uygulamalara cevap veremeyeceği kadar hızda çok büyük miktarlarda veri gönderilmesidir. Bu durum iletimin ve yanıt sürelerinin yavaşlamasına veya bir cihazın ya da hizmetin kilitlenmesine neden olmaktadır.
- Kötü amaçlı biçimlendirilmiş paketler: Saldırgan tarafından bir ağa, sunucu bilgisayarlarına veya uygulamalara bir veri paketi gönderilir, ancak alıcı bu veriyi işleyememesi nedeniyle istemci bilgisayarının yavaş çalışması veya kullanım dışı kalması gibi sonuçlar doğmaktadır.

DoS saldırıları bilgisayar ağlarındaki veri iletişiminde aksamaya sebep olduklarında bireyler ve kurumsal şirketler için zaman ve para kaybına neden olacakları için büyük bir risk faktörü olarak görülmektedir (Sharafaldin ve ark., 2018). Genellikle bu saldırıların profesyonel olmayan yeni başlamış saldırganlar tarafından yapılması oldukça kolaydır.

DoS saldırıları genelde açık sistem ara bağlantısı (Open System Interconnection-OSI) katmanlarından gerçekleşmektedir (Ajayi ve ark., 2022). Bunlardan özellikle uygulama katmanında yapılan DoS saldırıları genellikle kendilerini ağ düzeyinde göstermediğinden geneleksel ağ katmanı tabanlı saldırı tespit sistemlerinden kaçınabilmektedir. Bu nedenle siber güvenlik araştırma topluluğu, özel olarak uygulama katmanı DoS saldırılarını algılama ve azaltma mekanizmalarına odaklanmaktadır. Ancak, bu saldırılara karşı güvenilir ve verimli savunma mekanizmalarının oluşturulması için, siber güvenlik araştırmacıları tarafından uygulama katmanında yapılan DoS saldırılarının kapsamlı bir şekilde anlaşılması gerekmektedir. Şekil 1'de örnek bir DoS saldırısı gösterilmiştir.



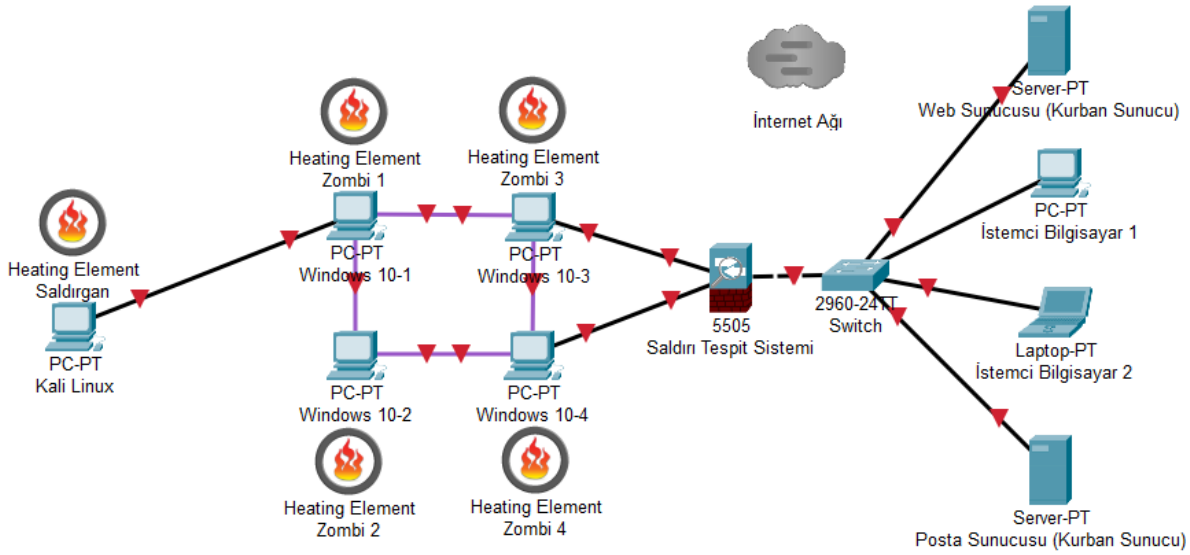
Şekil 1. Örnek bir DoS saldırı senaryosu.

Şekilde görüldüğü üzere gibi Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan dört masum kullanıcı bilgisayarından bir tanesine saldırmaktadır. Bu sayede kurban bilgisayar kullanıcısının iş yapamaz ve çalışamaz duruma gelmesi ve devre dışı kalması sağlanmıştır.

4.2. Dağıtık Hizmet Reddi Saldırısı

DDoS genellikle büyük ölçekte gerçekleştirilen ve anlık istekler göndererek servis sağlayıcısının kaldırabileceği yükün çok üzerinde kaynakları tüketerek sunduğu servislerin tamamen durmasına neden olan bir saldırı olarak tanımlanmaktadır (Akgun ve ark., 2022).

DDoS saldırısı saldırganlar tarafından bireysel kullanıcılar, kurumsal şirketler ve devlet kurumlarına ait web sunucusu kaynaklarına karşı yapılarak son kullanıcı istemcilerinin erişimini azaltmak veya engellemek amacıyla zombi adı verilen birden çok istemci bilgisayar ile yapılmaktadır. Bu süreçte virüs bulaşmış istemci bilgisayarlar zombi olarak adlandırılır. Zombi bilgisayarlar, her zaman yerel ağda virüs bulaştıracak istemci bilgisayarlar arayarak ve bu bilgisayarlara virüs bulaştırarak daha fazla zombi bilgisayarlar yaratmakta ve ağını genişletmektedir. Bu nedenle yüzlerce hatta bazen binlerce bilgisayar tarafından gerçekleştirilen DDoS saldırılarını zamanında tespit edip engelemek oldukça zor bir süreçdir (Taner, 2019). Şekil 2'de örnek bir DDoS saldırısı gösterilmektedir.



Şekil 2. Örnek bir DDoS saldırı senaryosu.

Şekilde görüldüğü üzere Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden sızma aracılığıyla ele geçirdiği bilgisayarlar ile kendisine yeni bir zombi ağı oluşturmuştur. Daha sonra bu zombi bilgisayarlar farklı zamanlarda IDS'yi geçerek yerel ağda bulunan web sunucusu veya mail sunucusuna taşıyamayacağı kadar veriyi gönderip sunucunun devre dışı kalmasını sağlayarak ağda bulunan istemci bilgisayar kullanıcılarının sunuculardan hizmet alamamasına ve web/mail sistemlerinin devre dışı kalmasına neden olmuştur.

Web sunucuları birçok nedenden dolayı çevrimdışı olabilmektedir (Singh ve ark., 2018). Bunun en önemli nedenlerinden biri de web sunucusuna yapılan DDoS saldırılarıdır. Bu saldırılar yalnızca sunucu kaynaklarını tüketmekle kalmaz, aynı zamanda normal istemcilere de zarar verebilir. Bu nedenle, DDoS saldırılarının tespiti mevcut araştırmacıların birincil hedeflerinden biri haline gelmektedir.

Web sunucularında yapılan DDoS saldırıları genel olarak OSI katmanlarındaki ağ katmanı ve taşıma katmanına yapılan saldırılar olmak üzere ikiye ayrılmaktadır. Ağ katmanındaki DDoS saldırısı internet kontrol mesajı protokolü (Internet Control Message Protocol-ICMP) veya kullanıcı datagram protokolü (User Datagram Protocol-UDP) portlarından yapılırken taşıma katmanındaki ise taşıma kontrol protokolü (Transmission Control Protocol-TCP) portlarındaki sistem açıklıklarından sızarak gerçekleştirilmektedir.

Son yıllarda internete bağlanan cihazların sayısı giderek artmaktadır. Ancak bu artışı sadece bilgisayar kullanımının yaygınlaşması ile ifade etmek yanıltıcı olabilir. Çünkü günümüzde bilgisayarların yanı sıra nesnelerin interneti (Internet of things-IoT) olarak tanımlanan cihazların kullanımındaki artış yatsınamayacak kadar büyüktür. Bu yaygınlaşma, DDoS saldırılarının da kendi içinde yüksek ve düşük oranlı DDoS saldırıları olarak

ayrılmasına neden olmuştur. Yüksek oranlı DDoS saldırıları genellikle sunucu sistemlerine yapılırken düşük oranlı DDoS saldırıları ise diğer internete bağlı nesnelere yönelik gerçekleştirilmektedir (Toklu ve ark., 2018).

DDoS saldırıları, en yaygın siber tehdit biçimi haline gelmekte olup her geçen yıl hem sayı hem de hacim olarak artmaktadır. Temel motivasyon kaynağının finansal kazançlar olduğu ifade edilen DDoS saldırılarının özellikle kurumsal web siteleri veya bankaların internet servis sağlayıcıları üzerinde odaklandığı söylenebilir (Kumari ve ark., 2023).

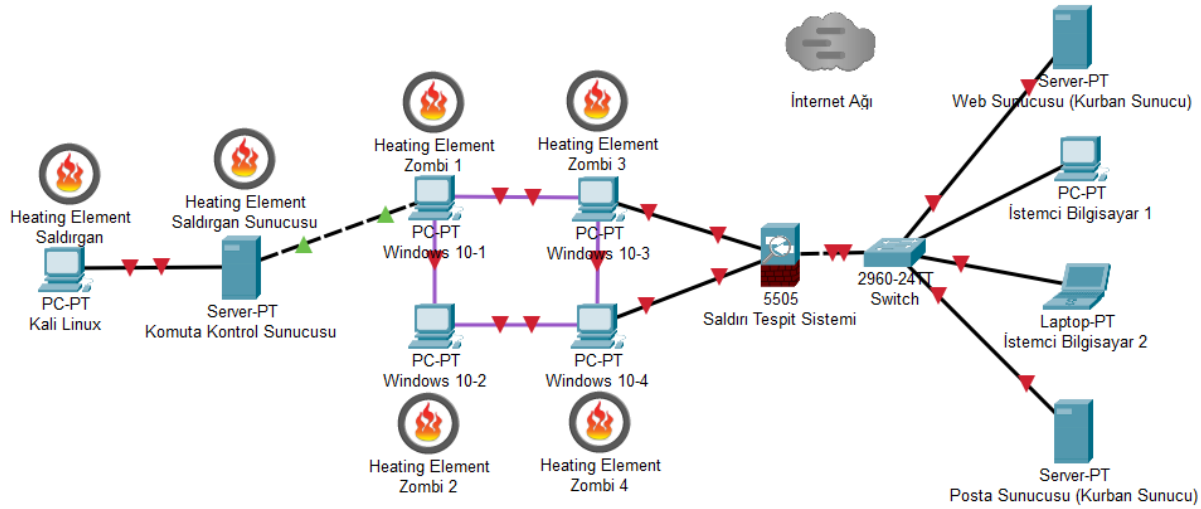
4.3. Botnet Saldırısı

Botnet saldırısı bir birey veya bir grup saldırgan tarafından kontrol edilen ve internet üzerinden birbirine bağlanmış bilgisayarlar vasıtası ile yapılmaktadır. Botnet saldırısına maruz kalan bilgisayarlar, virüslü bir medya dosyasını veya bir spam e-posta ekini açarak ya da zararlı bir web sitesini ziyaret ederek enfekte olurlar. Bir başka deyişle, botnet, bir komuta ve kontrol bilgisayarı ile botnet ağındaki diğer bilgisayarların yönetilmesi olarak tanımlanmaktadır (Rumsey ve ark., 2016). Saldırgan öncelikli olarak masum kullanıcıya ait bilgisayarın kullanıcı adı ve şifresini ele geçirerek kendi ağındaki komuta ve kontrol sistemindeki botnet ağına dâhil eder. Saldırgan kendi ağındaki bilgisayarları komuta ve kontrol bilgisayarı aracılığı ile aynı anda bir DDOS veya kaba kuvvet saldırısı yapmak için kullanabilir. Hatta siber suçlular botnet bilgisayarlarını siber saldırılar gerçekleştirilmesi için üçüncü şahıslara kiralayabilirler.

Bot bilgisayarlar kullanıcıların bilgisi olmadan ve kullanıcı farkına varmadan çalışmaları nedeniyle genellikle tespit edilemezler. Botnet saldırılarına karşı antivirüs programları kullanılarak ve web tarayıcılarının açıklıklarını kapatarak önlem alınabilir. Genellikle botnet saldırıları aşağıdaki özellikleri sergilerler (Taner, 2019):

- Zararlı yazılım barındıran bilgisayarlar internet ağı aracılığı ile bir komuta ve kontrol bilgisayarına bağlıdır,
- Web/posta sunucusu çökmeden önce sistem yöneticisine IDS ile uyarı logları gönderilir,
- Web/posta sunucusu üzerinde veya kurban bilgisayarda bilinmeyen dosyalar, programlar veya masaüstü simgeleri vardır,
- Web/posta sunucusu üzerinde veya kurban bilgisayarda bulunan uygulamalar kendilerini kapatıyor ya da yeniden kendilerini konfigüre ediyorlardır,
- Kullanıcının izni olmadan spam e-postalar gönderiliyordur.

Şekil 3'te örnek bir botnet saldırısı gösterilmiştir.



Şekil 3. Örnek bir botnet saldırı senaryosu.

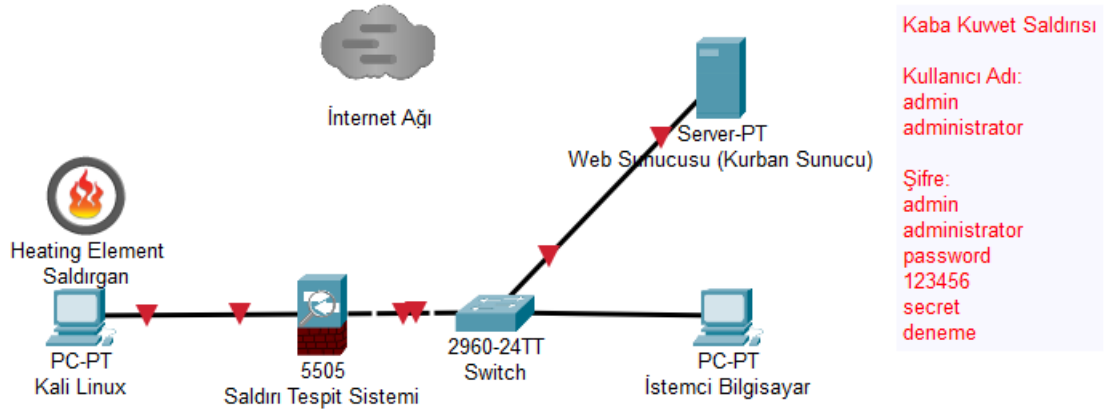
Şekilde gösterildiği gibi Kali Linux bilgisayarına sahip bir saldırgan internet ağında sızma ile ele geçirdiği bilgisayarlar üzerinden kendisine yeni bir botnet ağı kurmuştur. Saldırgan, komuta kontrol sunucusu üzerinden botnet ağında bulanan aktif zombi bilgisayarlarına web/posta sunucusuna atak yapılmak üzere aynı anda saldırı

emri verir. Bu süreçte IDS'yi aşarak ağda bulunan sunucuların kaynaklarını tüketerek istemcilerin hizmet alamamasına sebep olur.

4.4. Kaba Kuvvet Saldırısı

İnternet ağı üzerinden web tarayıcıları aracılığı ile kurumsal şirketlerin ve devlet kurumlarının hizmet verdiği web sayfalarının yönetim paneli giriş bilgilerinin, siber saldırganlar tarafından deneme ve yanılma yöntemi ile çok sayıda kombinasyon denenerek ele geçirilmesidir. Web sayfası yöneticileri tarafından oluşturulan yönetim paneli kullanıcı adı ve parola bilgileri harf, rakam ve özel karakterlerden oluşmaktadır. Bu bilgiler ne kadar karmaşık ve zor olursa kaba kuvvet ataklarına karşı daha dayanıklı olurlar. Bu saldırganlar başarılı olduklarında şirket hakkında hassas bilgilere erişirler. Ayrıca web sayfası aracılığı ile reklam spam'lerine ve şirket saygınlığının zarar görmesine neden olurlar.

Kaba kuvvet saldırısı, siber saldırganlar tarafından en fazla kullanılan ataklardan biridir. Genelde bu atak türü oturum açmak için gerekli olan kullanıcı adı ve şifreyi deşifre etmek için kullanılmaktadır. Ek olarak web sayfası uygulamaları aracılığı ile gizli sayfalarda kullanılan bilgileri keşfetmek için de kullanılmaktadır (Sharafaldin ve ark., 2018).
Eylül 2017 yılında McAfee Labs tarafından yayımlanan üç aylık raporda, kaba kaba kuvvet saldırısının kuvvet saldırılarının toplam ağ saldırılarının içerisinde yaklaşık olarak %20'sini oluşturduğu ve bu saldırıların web sayfası tabanlı güvenlik açıklarıyla yapıldığı belirtilmiştir (Salamatian ve ark., 2019). Şekil 4'te örnek bir kaba kuvvet saldırısı gösterilmiştir.

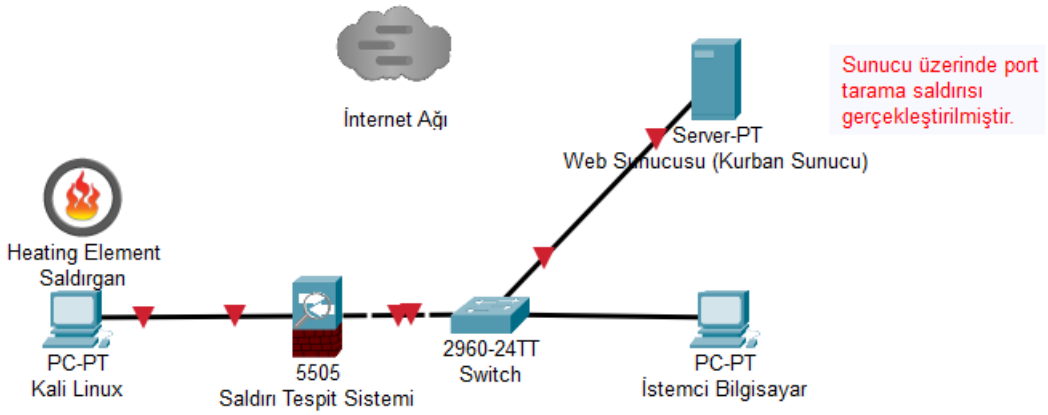


Şekil 4. Örnek bir kaba kuvvet saldırı senaryosu.

Şekilde gösterildiği üzere Kali Linux bilgisayarına sahip bir saldırgan, internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan web sunucuna ait web sayfası yönetim paneli kullanıcı adı ve şifresi için algoritmik kombinasyonlar deneyerek bilgileri ele geçirmiştir. Bu bilgiler ele geçirildikten sonra sunucu üzerinde yönetici yetkisine sahip olan saldırgan sunucuda bulunan verileri farklı bir sisteme aktarabilir ve sunucuyu kötü niyetleri için kullanabilir.

4.5. Port Tarama Saldırısı

Port tarama saldırısı gerçekleştirmek isteyen saldırgan, internet ağı üzerinden istemci bir bilgisayarın web sayfası aracılığı ile açık olan bir portu kullanarak ağa girer. Ardından ağ içerisinde istemci bilgisayarlar veya hizmet veren sunucuların içerisinde port taraması yaparak açık olan portları tespit eder. Genellikle bilgisayar sistemlerinde bilgisayar portları açık, kapalı ya da filtrelenmiş olarak gruplandırılırlar. Port tarama saldırısı yaygın olarak web tarayıcılarında taşıma katmanı güvenliğinde kullanılan güvenli şifreleme yöntemi olan OpenSSL şifreleme uygulaması açıklıklarından gerçekleştirilmektedir (Jacob ve ark., 2022). Şekil 5'te örnek bir port tarama saldırısı gösterilmiştir.



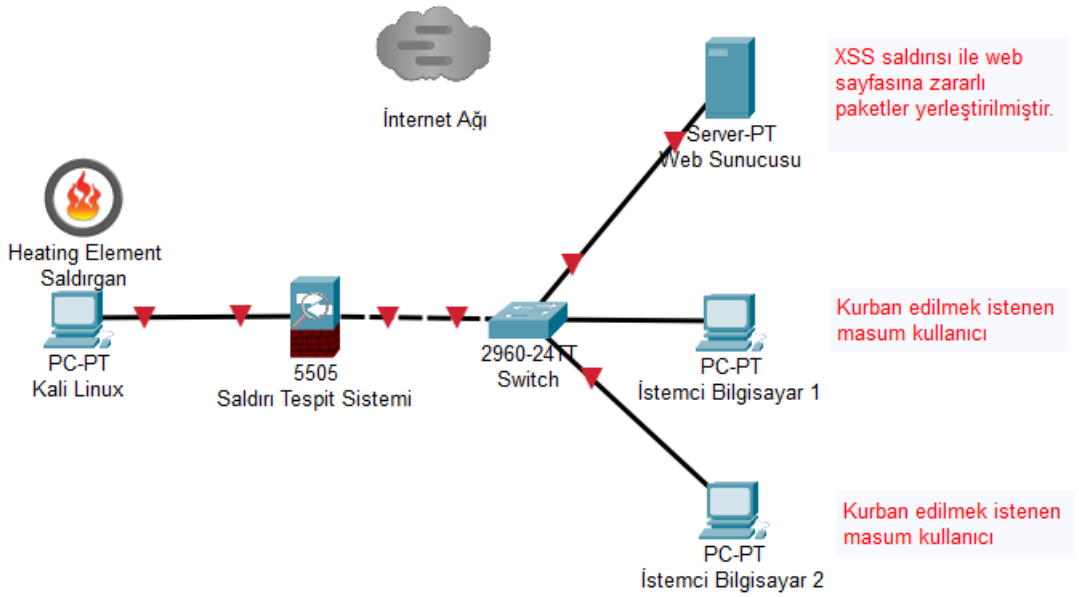
Şekil 5. Örnek bir port tarama saldırı senaryosu.

Şekilde gösterildiği gibi Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan istemci bilgisayar veya web sunucusuna ait açık portları bulmaktadır. İstemci bilgisayar veya web sunucusu içerisine girip kendisine yönetici yetkileri vererek istemci bilgisayar veya web sunucusunda bulunan verileri farklı bir sisteme aktarabilir ve bu sistemleri kötü amaçları için kullanabilir.

4.6. Web Uygulama Saldırısı

OWASP (Open Web Application Security Project) web uygulamalarındaki güvenlik açıklarının tespit edilerek kapatılması ve web uygulamaların güvenli bir şekilde korunmasını sağlamak için çalışmalar yapan bağımsız bir kuruluştur. OWASP 2018 yılında yayınladığı QWASP-Top 10 raporunda yer alan bilgilere göre SQL enjeksiyon (SQL injection) ve komut dosyası çalıştırma (Cross-Site Scripting-XSS) saldırısı en riskli güvenlik açıklıklarıdır.

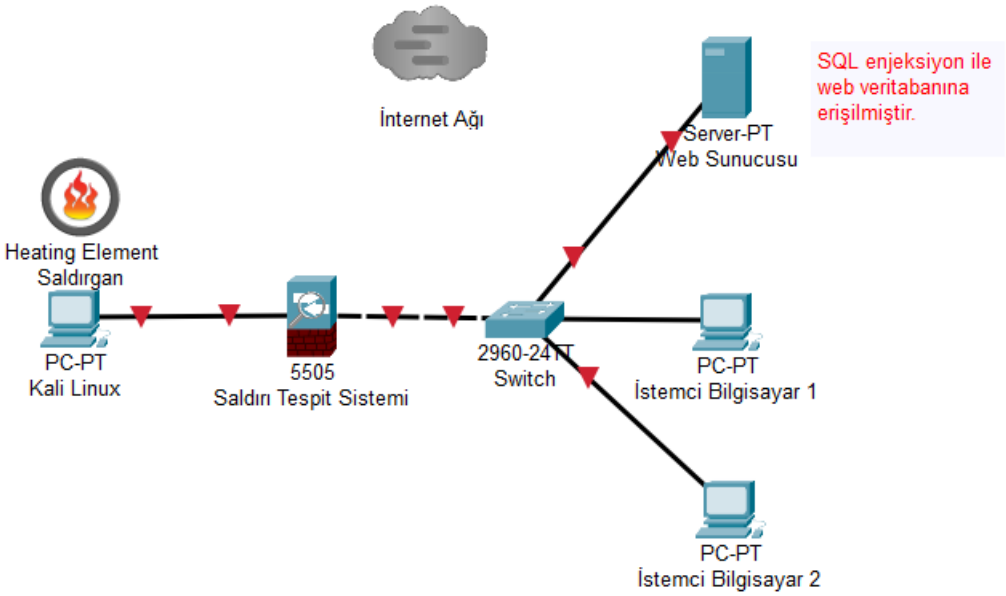
XSS saldırısında, saldırgan yoğun olarak kullanılan bir web sayfasına kötü amaçlı kod ilave eder ve kurbanın web tarayıcısında farkında olmadan kötü amaçlı komut dosyaları çalıştırmasına neden olur (Tariq ve ark., 2021). Saldırı, kurbanın kötü amaçlı kodu yürüten web sayfasını ziyaret etmesi ile gerçekleşir. Böylece web sayfası kötü amaçlı komut dosyasını kullanıcının tarayıcısına iletmek için bir araç haline gelmiş olur. Forumlar, mesaj panoları ve yorumlara izin veren web sayfaları XSS saldırıları için kullanılan savunmasız araçlara örnek olarak verilebilir. Şekil 6'da örnek bir XSS saldırısı gösterilmektedir.



Şekil 6. Örnek bir XSS saldırı senaryosu.

Şekilde görüldüğü üzere Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden IDS'yi geçmektedir. Ağda bulunan web sunucusu üzerinde hizmet veren web sayfasında saldırgan tarafından yerleştirilmiş zararlı kodlar bulunmaktadır. Masum olan bilgisayar kullanıcısı web sayfasından hizmet almak istediğinde sayfa içerisine gizlenmiş zararlı kodu çalıştırır ve zararlı kodlarda bulunan virüsü kendi bilgisayarına enjekte etmiş olur. Böylece kullanıcı, bilgisayarında bulunan verileri kendi rızası ve bilgisi olmadan dışarıya aktarmış olmaktadır.

SQL enjeksiyon, web uygulamalarında bulunan veri tabanlarını hedefleyen bir saldırı türüdür (Kasim, 2021). Bu saldırı türü SQL komutlarını kullanılarak gerçekleştirilmektedir. SQL sorguları ile web uygulamalarının arkasındaki veri tabanı sunucuları kontrol edilmektedir. Genellikle saldırganlar, web sunucusu veri tabanında yer alan verileri değiştirebilir veya silebilir, bu da uygulamanın içeriğinde veya davranışında kalıcı değişikliklere sebep olur. Sonuç olarak devlet kurumları ve kurumsal işletmeler itibar kaybına ve finansal kayıplara uğrayabilir (Crespo-Martínez ve ark., 2023). Şekil 7'de örnek bir SQL enjeksiyon saldırısı gösterilmiştir.



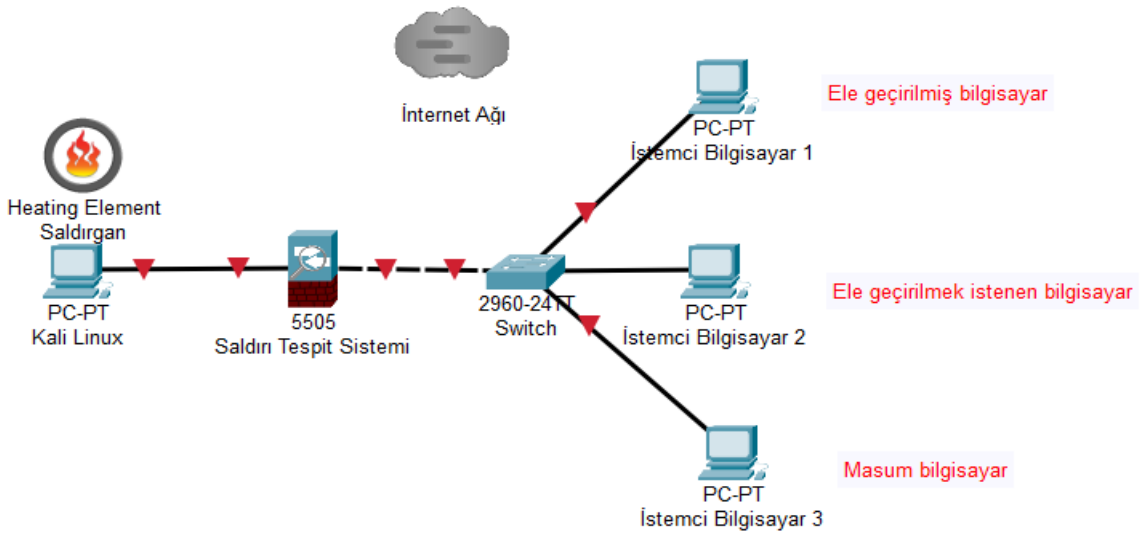
Şekil 7. Örnek bir SQL enjeksiyon saldırı senaryosu.

Şekilde gösterildiği gibi Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan web sunucusu üzerinde bulunan web veri tabanına sızmaktadır. Saldırgan kendisine yönetici yetkilerini vererek veri tabanında bulunan verileri değiştirebilir ve silebilir. Bunun sonucunda hizmet alan istemci bilgisayarlar veri tabanından hizmet almak istediğinde değişmiş veya silinmiş bilgilerle karşılaşarak hizmet eksikliğine yol açılmış olur.

XSS, web uygulamalarını kullanan kullanıcıları hedefleyen güvenlik açığı iken SQL enjeksiyon, web uygulamaları tarafında kullanılan veri tabanlarındaki güvenlik açıklıklarını hedeflemektedir.

4.7. Sızma Saldırısı

Sızma saldırısı (infiltration), ağa sızma olarak bilinen ve savunmasız bir yazılımdan yararlanılarak gerçekleştirilen bir saldırı türüdür. Örneğin saldırganlar tarafından adobe acrobat reader veya dropbox gibi yaygın olarak kullanılan programların kullandığı portlar üzerinden sızma gerçekleştirilir. Saldırganlar sızma gerçekleştikten sonra bilgisayarın tespit edilen portlarından kolaylıkla önce bilgisayara daha sonra yerel ağa giriş ve çıkış yapabilir. Bu portlar aracılığı ile bilgisayar üzerinden farklı saldırılar gerçekleştirebilir. Ayrıca saldırganlar, NMap kullanarak yerel ağ üzerinde IP taraması yapabilir, ağ içerisindeki diğer açıklıkları tespit edebilir ve ağ cihazlarına/sunuculara ataklar gerçekleştirebilir. Şekil 8'de örnek bir sızma saldırısı sunulmaktadır.



Şekil 8. Örnek bir sızma saldırı senaryosu.

Şekilde gösterildiği gibi Kali Linux bilgisayarına sahip bir saldırgan, internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan istemci bilgisayarlardan bir tanesine üçüncü paket programların kullandığı port ile sızmış olup, daha sonra ağda bulunan diğer masum bilgisayarları ele geçirmek istemektedir.

5. SONUÇLAR

Günümüzde bilgi teknolojileri hızla gelişirken bilgisayarların ve IoT cihazlarının daha da yaygınlaşacağı ve siber saldırganlar tarafından yeni saldırı yöntemlerinin geliştirileceği düşünülmektedir. Bu nedenle yeni siber saldırılar, hizmet alan son kullanıcılar tarafından büyük bir kaygı ve endişe yaratmış olacaktır. Bu süreçte ağ güvenlik duvarlarından olan IDS ve IPS'lere önemli roller düşecektir. Bu çalışmada öncelikli olarak ağ güvenlik duvarları ve ağ saldırıları tanımlandıktan sonra ağ ortamında gerçekleşen saldırı türlerlerinden olan DoS, DDoS, botnet, kaba kuvvet, port tarama, web uygulama ve sızma ataklarına yer verilmiştir. Her bir saldırı türü için örnek senaryolar oluşturulmuş ve senaryolar açıklanmıştır.

KAYNAKLAR

Ajayi, O., Gangopadhyay, A., Erbacher, R. F., & Bursat, C. (2022). Developing Cross-Domain Host-Based Intrusion Detection. Electronics, 11(21), 3631.

Akgun, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security, 118, 102748.

Crespo-Martínez, I. S., Campazas-Vega, A., Guerrero-Higueras, Á. M., Riego-DelCastillo, V., Álvarez-Aparicio, C., & Fernández-Llamas, C. (2023). SQL injection attack detection in network flow data. Computers & Security, 127, 103093.

Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE.

Jacob, S., Qiao, Y., Ye, Y., & Lee, B. (2022). Anomalous distributed traffic: Detecting cyber security attacks amongst microservices using graph convolutional networks. Computers & Security, 118, 102728.

James, F. (2019, October). IoT cybersecurity based smart home intrusion prevention system. In 2019 3rd Cyber Security in Networking Conference (CSNet) (pp. 107-113). IEEE.

Kasim, Ö. (2021). An ensemble classification-based approach to detect attack level of SQL injections. Journal of Information Security and Applications, 59, 102852.

Kumar, A., Abhishek, K., Ghalib, M. R., Shankar, A., & Cheng, X. (2022). Intrusion detection and prevention system for an IoT environment. Digital Communications and Networks, 8(4), 540-551.

Kumari, P., & Jain, A. K. (2023). A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures. Computers & Security, 103096.

Rumsey, M. J. (2016). Cybersecurity: Challenging rhetoric to identify the future of defensive and offensive measures against defined threat actors (Doctoral dissertation, San Diego State University).

Salamatian, S., Huleihel, W., Beirami, A., Cohen, A., & Médard, M. (2019). Why botnets work: Distributed brute-force attacks need no synchronization. IEEE Transactions on Information Forensics and Security, 14(9), 2288-2299.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, 108-116.

Singh, K. J., Thongam, K., & De, T. (2018). Detection and differentiation of application layer DDoS attack from flash events using fuzzy-GA computation. IET Information Security, 12(6), 502-512.

Tams, B., Mihăilescu, P., & Munk, A. (2015). Security considerations in minutiae-based fuzzy vaults. IEEE Transactions on Information Forensics and Security, 10(5), 985-998.
Taner, C. (2019). Herkes için Siber Güvenlik, Abaküs Kitap.

Tariq, I., Sindhu, M. A., Abbasi, R. A., Khattak, A. S., Maqbool, O., & Siddiqui, G. F. (2021). Resolving cross-site scripting attacks through genetic algorithm and reinforcement learning. Expert Systems with Applications, 168, 114386.

Toklu, S., & Şimşek, M. (2018). Two-layer approach for mixed high-rate and low-rate distributed denial of service (DDoS) attack detection and filtering. Arabian Journal for Science and Engineering, 43(12), 7923-7931.

İNTERNET KAYNAKLARI

OWASP (Open Web Application Security Project), https://owasp.org/, Son Erişim Tarihi 22 Mayıs 2023.

Cisco Ağ Akademisi CCNA1 CCNAv7: Introduction to Networks, https://contenthub.netacad.com/itn/16.1.1, Son Erişim Tarihi 22 Mayıs 2023.

TEŞEKKÜR ve BEYANLAR

Yazarlar çalışmaya eşit oranda katkı sağlamıştır. Bu çalışmada herhangi bir potansiyel çıkar çatışması bulunmamaktadır. Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

Not: *Bu makale, Milli Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, Siber Güvenlik Tezli Yüksek Lisans Programı'nda, Doç. Dr. Can EYÜPOĞLU danışmanlığında, Fırat KILINÇ tarafından yürütülecek olan, "Makine Öğrenmesi Yöntemleri Kullanılarak Saldırı Tespiti" başlıklı yüksek lisans tezinin ön çalışmalarından yararlanılarak hazırlanmıştır.*