BMBAD BJESR Mühendislik Bilimleri ve Araştırmaları Dergisi
Journal of Engineering Sciences and Researches

Ağ Sistemlerinin Güvenliği İçin Siber Saldırıların Ayrık Olaylı Sistem Tanımlama Tabanlı Modellenmesi ve Simülasyonu

Discrete Event System Identification Based Modeling and Simulation of Cyber Attacks for the Security of Network Systems

[1]Şahin KARA, [2]Ahmet ZENGİN, [3]Selman HIZAL

[1]*Sakarya Uygulamalı Bilimler Üniversitesi, KSSMYO, Kaynarca/Sakarya, Türkiye*
[2]*Sakarya Üniversitesi, Bilgisayar ve Bilişim Bilimleri Fakültesi, Serdivan /Sakarya,*
[3]*Sakarya Uygulamalı Bilimler Üniversitesi, Teknoloji Fakültesi, Serdivan /Sakarya, Türkiye*

[1]sahinkara@subu.edu.tr, [2]azengin@sakarya.edu.tr, [3]selmanhizal@subu.edu.tr

Araştırma Makalesi/Research Article

ARTICLE INFO

Article history

Received : 20 March 2023
Accepted : 21 April 2023

Keywords:

Cyber Attack Experiments, Cyber Security, Simulation And Modeling, DEVS.

ABSTRACT

The rapid progress in information and network technologies has made these technologies indispensable tools both for individuals and in all areas of corporate functioning. This obligatory situation created by this development has brought risks and threats. Although many attack detection and prevention systems have been developed against cyber-attacks, vulnerability violations are increasing. In this study, it is aimed to develop a software-based tool to identify security vulnerabilities and detect cyber-attacks. In order to reduce test time and costs, the effective results of performing attack simulation experiments on virtual networks instead of real systems have been achieved with sample applications. As a case study, a cyber-attack simulation model and application based on the DEVS formalism has been developed. This tool provides a suitable infrastructure for modeling and simulation of more different cyber-attack scenarios in future studies.

MAKALE BİLGİSİ

Makale Tarihleri

Gönderim : 20 Mart 2023
Kabul : 21 Nisan 2023

Anahtar Kelimeler:

Siber Saldırı Deneyleri, Siber Güvenlik, Simülasyon Ve Modelleme, DEVS.

ÖZET

Bilişim ve ağ teknolojilerindeki hızlı ilerleme, hem bireyler için hem de kurumsal işleyişin her alanında bu teknolojileri vazgeçilmez birer araç haline getirmiştir. Bu gelişme ile oluşan bu zorunlu durum, beraberinde risk ve tehditleri de getirmiştir. Siber saldırılara karşı, pek çok saldırı tespit ve engelleme sistemleri geliştirilmesine rağmen zafiyet ihlalleri de artmaktadır. Bu çalışma ile güvenlik zafiyetlerinin belirlenmesi ve siber saldırıların tespit edilmesi için yazılım tabanlı bir araç geliştirilmesi amaçlanmıştır. Test zamanını ve maliyetleri düşürmek için gerçek sistemler yerine sanal ağlarda saldırı simülasyon deneyleri yapmanın etkili sonuçlarına örnek uygulamalarla ulaşılmıştır. Bir vaka çalışması olarak, belirli saldırı senaryoları için DEVS formalizmine dayalı bir siber saldırı simülasyon modeli ve uygulaması açık kaynak kodlu olarak geliştirilmiştir. Bu araç, sonraki çalışmalarda daha farklı siber-saldırı senaryolarının modellenmesi ve simülasyonu için uygun bir altyapı sağlamaktadır.

ORCID ID: [1]0000-0001-8736-2730
[2]0000-0003-0384-4148
[3]0000-0001-6345-0066

1. GİRİŞ

Bilgisayar ağ sistemlerinin güvenliği gün geçtikçe daha kritik bir güvenlik problemi olarak karşımıza çıkmaktadır. Günümüzde bütün teknolojik donanımlar ve onları çalıştıran yazılımlar ile cihazları birbirine bağlayan iletişim ağlarından oluşan siber ortamın hemen hemen her alanda kullanılması siber ortam güvenliğini önemli ve yüksek öncelikli bir konu durumuna getirmiştir. Güvenliğe verilen önem artmış olsa bile, sistemler bugün artık daha açık ve saldırıya maruz kalma ihtimalleri de daha yüksektir. Bireyeler, kurumlar ve devletler, yüksek miktarda önemli verilerini siber ortamda bulundurmaktadır. Bu durum kötü niyetli siber saldırganları farklı amaçlarla harekete geçiren bir motivasyon kaynağı olmaktadır. Siber saldırıları gerçekleştirmek için kullanılan uygulamalar kolaylıkla elde edilebilmektedir. Bu saldırıların zararlarından korunmak için pek çok saldırı tespit sistemi geliştirilmiştir. Bu çalışmalar, bilişim sistemlerine yönelik saldırı ve güvenlik ihlallerini tam engellemek için yeterli olamamaktadır [1]. Hedef alınan siber ortamlara yönelik siber saldırı gerçekleştirmek isteyen tarafların hedeflerine ulaşmak için başvurabilecekleri pek çok siber saldırı yöntemi mevcuttur. Bilgisayar ağlarındaki tüm güvenlik açıklarını bulmak ve çeşitli güvenlik önlemlerini güncel tutmak şirket ağ yöneticileri için zorlu bir süreçtir. Bu durum, ağa saldırmayı planlayanlar için bir avantaja dönüşmektedir [2].

Genel güvenlik politikaları her organizasyon için yeterli koruma sağlayamadığı için ek güvenlik önlemlerine ihtiyaç vardır. Bilgi veya mali kayıplara tahammülü olmayan kurumlar için en küçük bir risk bile çok hayati olabilmektedir. Olası tüm istismar yollarını minimuma çekmek için sürekli güvenliği ihlal edilmiş varlıkları açığa çıkaran kapsamlı senaryolar çalıştırılmalıdır. Bu amaçla siber saldırı simülatörlerinden (benzetim araçları) faydalanmak önemli kolaylıklar sağlamaktadır. Gerçek sisteme erişmek kolay olmayan durumlarda ve gerçek bir sistemde deney yapmak tehlike arz ediyorsa bununla birlikte gerçek sistemlerde deney yapmak ekonomik olmuyorsa, simülasyon en genel geçer model olmaktadır. Siber saldırı simülasyonunun sonucu, organizasyonun nerede risk altında olduğunu görmek ve düzeltmek maksadıyla harekete geçmek için saldırganın bakış açısından olası her saldırı yolu ve saldırı vektörü türü kontrol edilebilmektir.

Mevcut siber saldırı simülatörlerinin bir kısmı iyi tasarlanmadığı için bilgisayar ağı benzetiminde ağ ve ağ bileşenleri çok az ve sınırlı bilgi içermenin yanı sıra saldırıya özgü uygun IDS uyarı çıktıları üretememektedir ve bazı saldırı adımları tamamen göz ardı edilmektedir. Bir kısım simülatörler saldırı projeksiyonunu daha büyük bir sistemin parçası olarak kullanmakta ve araştırma çalışmaları siber saldırılara tam olarak odaklanmamaktadır. Bazı siber saldırı modelleme sistemleri yalnızca yazılım korumasını test etmek için geliştirilmiştir, bağımsız sistem saldırılarını modellemede eksik kalmıştır. Literatür incelemesinde ilgili simülatörler tanıtılıp zayıf yönleri analiz edilmiştir.

Bu çalışmanın amacı, bilgisayar ağlarında veri güvenliğini sağlamak için siber saldırıların ve güvenlik tehditlerinin değerlendirilmesi ve yeni yöntemler geliştirilmesine olanak sağlayan bir simülasyon aracını geliştirmektir. Aynı zamanda siber saldırı verilerini elde ederek saldırı tespit sistemlerinin performans ve doğruluğunu arttırmak için bir simülasyon modelin geliştirilmesi amaçlanmıştır. Bu çalışmada siber güvenliğin sağlanması için en önemli aşama olarak güvenlik zafiyetlerinin ve açıklıkların kötü niyetli siber saldırganlardan önce bulunup önlem alınması amacıyla modelleme ve simülasyon araçlarının kullanıldığı bir uygulama geliştirilmiştir. Bu simülasyon aracını geliştirmek için Java, DEVS modelleme yaklaşımı ve DEVS-Suite yazılımı kullanılmıştır. DEVS, yaygın olarak kullanılan kapsamlı bir simülasyon alanıdır. DEVS, fiziksel sistemlerin davranışını, bilgisayar ağlarında olduğu gibi durumları zamanla değişen, zaman içinde etkileşime giren varlık koleksiyonlarını temsil etmeye ve incelemeye izin vermektedir. DEVS-Suite kullanılarak geliştirilen siber saldırı uygulaması, DEVS-Suite çekirdeğinin üzerine inşa edilmiştir. DEVS formalizmi ve ileri yazılım mühendisliği teknikleri kullanılarak üst düzey performans, ölçeklenebilirlik, teorik sistem tasarımı ve kullanım kolaylığı sağlanmaktadır.

Saldırı simülatörünün geliştirilmesi süreci belirli aşamalardan oluşmaktadır. Sistem tasarımı ve analizi için modelleme ve simülasyon hedeflerinin belirlenmesi kavramsal modelleme aşamasında gerçekleştirilmektedir. Temel ağ sentezi aşamasında geliştirilen varlıklar ve düğümler bağlanarak değişik topolojiler ve ağ konfigürasyonları oluşturulmuştur. Saldırı modelleme aşamasında saldırı modelleri kendi karakteristiklerine göre geliştirilerek deneysel çerçeveye eklenmiştir. Geliştirilen modellerin simülasyon deneyleri için DEVS deneysel çerçeve kavramı kullanılmıştır. Saldırı simülasyonu sürecinde saldırı simülasyon testleri yapılıp, sonuçlar gözlemlenip analizleri yapılmış ve grafikler oluşturulmuştur.

Çalışmanın giriş bölümünün ardından ilgili lireratür incelemesi; ikinci bölüm siber saldırı türleri ve sınıflandırma yöntemlerini içermektedir. Üçüncü bölüm siber saldırıların modellenmesini ve saldırı simülatörünün geliştirilmesi sürecini içermektedir. Dördüncü bölüm simülasyon deneylerini, son bölümde ise sonuçlar, değerlendirme ve gelecek çalışmalar yer almaktadır.

2. LİTERATÜR TARAMASI

Cohen'in siber saldırı simülatörü referans alınarak geliştirilen SECUSIM siber saldırı aracı, ilk siber saldırı sümülatörlerinden biridir [3,4]. Bu simülatörlerin her ikisi de saldırgan davranışı uygulamıştır. Ancak sonuçları önceden tanımlanmış saldırı adımlarına dayanmaktadır ve simülatörler belirli güvenlik açıklarını hesaba katmamakta ve uyarı çıktıları üretmemektedir. Kotenko ve Man'kov tarafından geliştirilen "Attack Simulator" siber saldırı aracında bilgisayar ağı benzetiminde ağ ve ağ bileşenleri çok az ve sınırlı bilgi içermektedir [5]. Kim

ve arkadaşları ağ güvenliği simülasyonu için bir DEVS modelleme yöntemi önermiştir. Ancak ağ modeli düğüm sayısı az (100) tutulmuştur, saldırı modeli olarak sadece solucan simülasyon modeli geliştirilmiştir [6].
Dougherty ve Gonslaves [7], yazılım korumasının test edilmesine yardımcı olmak için uyarlanabilir bir siber saldırı sistemi geliştirilmiştir. Bu araştırma yoluyla yapılan modelleme, yalnızca yazılım korumasını test etmek için geliştirilmiştir, bağımsız sistem saldırılarını modellemede eksik kalmıştır. Cheung ve ark. [8], saldırı senaryolarının gerçek IDS uyarılarını gözleyerek modellendiği "İlişkili Saldırı Modelleme" adlı bir projeyi geliştirmiştir. Birçok IDS uyarısı yanlış pozitif olabilmesi ve bazı saldırı adımları tamamen atlanmış olma ihtimali modelleme sürecini olumsuz etkileyebilmektedir. Holdender ve ark. [9], grafik teori tekniklerinden yararlanarak, diğer bazı saldırı türlerinin yapılabilmesi için hangi saldırı eylemlerinin veya istismarın gerekli olduğunu belirleyen bir grafik tabanlı şablon geliştirmiştir. Garg ve ark. [10], saldırıları tespit etmek amacıyla güvenlik mekanizmalarının yeteneklerini ölçmek için bir çerçeve geliştirmiştir. IDS'ler ve diğer güvenlik sistemleri, özellikle uyarı verileri gerektiren bir simülasyon için gerekli olandan çok daha karmaşık bir şekilde modellenmiştir. DeLooze ve ark. [11], siber saldırıların ve güvenlik sistemlerinin kombinasyonunu modellemek için bir simülasyon metodolojisi geliştirmiştir. Bu sistem, bir eğitim aracı olarak kurulduğundan, saldırılar ve IDS uyarılarıyla ilişkili veri üretimi için yeterli derecede iyi tasarlanmamıştır. Kistner [12], ağ aygıtları için daha ayrıntılı nitelikler geliştirmek ve bir dizi parametre temelinde saldırıları otomatik olarak üretmek için bir yöntem sağlamak için bu çalışmayı daha da genişletmiştir. Cohen [3] tarafından geliştirilen simülatör ilk simülatörlerden biri olup sonraki bazı çalışmalar bunun üzerine kurulmuştur. Kotenko ve Man'kov [5], tasarım ve dağıtım aşamalarında bilgisayar ağlarının güvenlik açığının aktif olarak değerlendirilmesi için tasarlanan "Attack Simulator" yazılım aracıyla ilgili uygulama sorunlarını ve deneylerini anlatmaktadır. Önerilen model varlıklara dayalı saldırı yapılandırması ve saldırı senaryolarının durum makinelerinin tanımlamalarına dayanmaktadır. Bu çalışmada bilgisayar ağı benzetiminde ağ ve ağ bileşenleri çok az ve sınırlı bilgi içermektedir. Ulanov ve Kotenko [13] internette yazılımsal ajanlardan oluşan ekiplerin ve aralarındaki siber savaş senaryolarının modelleme ve simülasyonu gerçekleştirilmiştir. Kuhl ve Sudit [14], siber güvenlik yöntemlerinin test edilmesi için uzun zaman gerektiren ve oldukça maliyetli olan fiziksel ağlara alternatif olarak sanal bir simülasyon modelleme yaklaşımı sunmaktadır. Bu simülatör, bir ağdaki paket akışının ayrıntılarını modelleyemez, ancak kötü niyetli siber saldırıları ve kötü amaçlı olmayan ağ etkinliğini temsil eden simüle edilmiş uyarılar üreterek izinsiz giriş tespit sisteminin davranışını simüle edebilir. Van Leeuwen ve ark. [15], ağ bilgi sistemleri ve iletişim ağlarının incelenmesi için bir siber güvenlik analiz ve deney ortamı geliştirmiştir. Bu simülasyon ortamı donanım destekli sanallaştırma gerektiren bir altyapı satın almayı ve kurmayı gerektirdiği için yüksek başlangıç maliyetlerine ve sınırlı büyüme esnekliğine sahiptir. Torres ve ark. [16], kablolu ve kablosuz tam ölçekli taktiksel sanal ağlarda siber saldırı ve güvenlik yöntemlerinin test ve analizini yapabilen, önceden yapılmış ilgili bazı çalışmalar üzerine kurulu yeni bir simülasyon ortam modeli sunmaktadır. Geliştirilen model ile bir dizi siber saldırı yapılarak belli bir sanal ağ mimarisinin esneklik ve sağlamlığı test edilebilmektedir. Norman ve ark. [17], siber alanda ağ sistemlerinin test ve deneylerinin geliştirilmesi için bir simülasyon modeli tasarlamıştır. Bu modelde karmaşık ağlarda hızlı ve düşük maliyetli analiz, siber saldırı/faaliyet etkilerini değerlendirmek, silah sistemleri üzerindeki siber etkinin değerlendirilmesi ve çeşitli tehdit ve hedef sistemlerin temsil edildiği simülasyon ortamı sunulmaktadır. Kotenko ve Chechulin [18], saldırganların tespiti ve bunlara karşı gerçek zamanlı önlemlerin belirlenmesi için siber saldırı grafikleri kullanarak güvenlik değerlendirmesi ve etki analizi sağlayan bir sistem olan CAMIAC'ı sunmuşlardır. Ancak sistem, saldırı projeksiyonunu daha büyük bir sistemin parçası olarak kullanmaktadır ve araştırma çalışmaları siber saldırılara odaklanmamaktadır.
Ekelhart ve ark. [19], güvenlik analizi neticesinde ortaya çıkan ve çeşitli düşmanlara karşı sistemin direncini deneysel olarak değerlendirmede nasıl kullanılabileceğini gösteren bir prototip uygulamayı tanımlamıştır. Bu çalışmada saldırı modelleri yeterince iyi modellenmemiştir, sosyal mühendislik, ağ oluşturma gibi ek davranış modelleri ve saldırı kalıpları eksik kalmıştır. Bergin [20], otonom araç sistemlerinde siber güvenliğin modellenmesi ve simülasyon desteği için bir siber saldırı ve savunma simülasyon yapısına olan ihtiyacı belirtmiştir. Bu otonom araç sistemleri insansız hava ve kara araçlarını kapsamaktadır. Örnek bir siber saldırı simülatör sistemi ile bu tip modelleri destekleyen bir yapı tanıtılmıştır. Park ve ark.[4], siber saldırı simülasyon aracı SECUSIM, saldırı mekanizmalarını belirlemek, savunma mekanizmalarını doğrulamak ve sonuçlarını değerlendirmek için Cohen'in siber saldırı simülatörünü referans alarak yeni bir araç geliştirmiştir. Bu simülatörlerin her ikisine de saldırgan davranışları uygulanmıştır. Ancak sonuçları önceden tanımlanmış saldırı adımlarına dayanmaktadır ve simülatörler belirli güvenlik açıklarını hesaba katmamış ve uyarı çıktıları üretmemiştir.
Ağ simülasyon araçlarının karşılaştırılması üzerine yapılan çalışmalar, siber saldırı simülatörlerine nispeten daha fazladır. Bu konuda yapılan literatür araştırmasında farklı siber saldırı simülasyon araçlarının senaryo sayıları, modellenebilir düğüm sayıları ve ağ türleri genel olarak karşılaştırılmıştır. Bu çalışmada, DEVS tabanlı siber saldırı simülatörü (DEVS-CAS) tanıtılmaktadır. Ayrıca yapmış olduğumuz performans analizlerinde bir bilgisayardaki diğer simülatörler ile 1500 düğüme ulaşmak mümkünken, DEVS-CAS ile yaklaşık 3000 - 3500 düğüme çıkarılabilmektedir. DEVS-CAS'ın daha iyi bir ölçeklenebilirliğe sahip olduğu söylenebilir. Bu tez çalışmasında geliştirilen siber saldırı simülatörünün diğer simülatörlerden daha iyi olan yönleri DEVS-Suite simülasyon yazılımının sağladığı esnek özelliklere dayanmaktadır.

3. SİBER SALDIRI TÜRLERİ

Literatüre baktığımızda, siber saldırı türlerini açıklamak ve tanımlamak için farklı metodolojiler ve sınıflandırmalar sunumuştur ve siber güvenlik uzmanlarının gelecekteki siber saldırıları tespit etme çalışmaları önem kazanarak devam etmektedir. Bu kapsamda bazı araştırmacılar, ağ ve bilgisayar saldırıları arasındaki ilişkiyi açıklamış ve araştırmalarında ek olarak siber saldırıları; saldırı türü, saldırının hedefi, zararlı güvenlik açıkları teknikleri ve faydalı yük saldırı türleri gibi dört boyuta ayırmıştır [21]. Burada faydalı yük, paketin, mesajın veya kodun verileri taşıyan kısmıdır. Bilgi güvenliğinde, faydalı yük terimi genellikle kötü amaçlı kodun yıkıcı işlemi gerçekleştiren kısmını ifade eder. Bazı araştırmacılar, saldırı türlerini, gelecek hedeflerini, sınıflandırmanın ölçümünü ve açıklamalarını anlatmak amacıyla siber saldırıların risk değerlendirmesine vurgu yaparak siber saldırıların bir sınıflandırmasını vermiş ve bilgisayar sistemlerindeki kusur ve zafiyetlerin kapsamlı bir analizini yapmışlardır [22]. Farklı araştırmacılar mobil bilgi işlem için güvenlik açıkları ve tehditlerin bir sınıflandırmasını, saldırının alt tipleri, işletim sistemi aygıtı üzerindeki etkisini, özel savunma tekniklerini ve verilen hasarları tanımlayan birçok farklı saldırı türünü açıklamıştır [23-26].

Tablo 1. Siber saldırı türleri.

Saldırı türü
Bilgi toplama ve keşif saldırısı
Virüs saldırıları
Truva atı ve arka kapı saldırıları
Solucan saldırıları
Port/bilgi tarama saldırısı
Sniffer (koklama) saldırıları
Numaralandırma saldırıları
Bilgi sistemi saldırıları
Tampon (arabellek) taşması saldırıları
Web sunucusu güvenlik açıkları saldırıları
İzinsiz giriş tespiti, ids, güvenlik duvarları ve honeypot saldırıları, arabellek taşması saldırıları
Sosyal mühendislik saldırıları
Hizmet reddi saldırıları
Oturum çalma saldırıları
Web tabanlı uygulama saldırıları
Kablosuz ağ saldırıları

Virüsler, kötü amaçlı yazılımlar, tuş kaydediciler (keylogger), arka planda çalışan gizli programlar (rootkit), casus yazılımlar, solucanlar, truva atları, hizmet reddi (DoS), dağıtılmış hizmet reddi (DDoS), ağ açıkları, uygulama saldırıları, kablosuz saldırılar, sosyal mühendislik, arabellek taşması ve ağ dinleme (sniffing) dahil olmak üzere farklı siber saldırı türlerini ayrıntılı olarak sunan ve öneren daha önceki çalışmalar da vardır [27-38]. Tablo 2.'de saldırı türleri gösterilmektedir.

4. SİBER SALDIRI YÖNTEMLERİNİN MODELLENMESİ

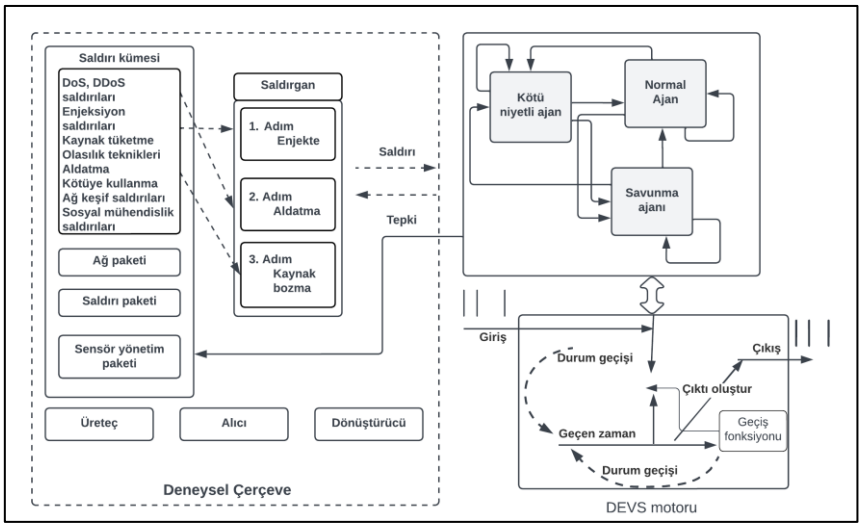
Saldırı simülatörünün geliştirilmesi süreci belirli aşamalardan oluşmaktadır. Sistem tasarımı ve analizi için modelleme ve simülasyon hedeflerinin belirlenmesi kavramsal modelleme aşamasında gerçekleştirilmektedir. Temel ağ sentezi aşamasında geliştirilen varlıklar ve düğümler bağlanarak değişik topolojiler ve ağ konfigürasyonları oluşturulmuştur. Saldırı modelleme aşamasında saldırı modelleri kendi karakteristiklerine göre geliştirilerek deneysel çerçeveye eklenmiştir. Geliştirilen modellerin simülasyon deneyleri için DEVS deneysel çerçeve kavramı kullanılmıştır. Saldırı simülasyonu sürecinde saldırı simülasyon testleri yapılıp, sonuçlar gözlemlenip analizleri yapılmış ve grafikler oluşturulmuştur. Bu çalışmada, DEVS-Suite altında topolojik olarak yapılandırılmış ve tasarlanmış sanal büyük ölçekli ağ sistemine karşı siber saldırı gerçekleştirmek için yaygın olarak kullanılan siber saldırı türleri modellenmiştir. Geliştirilen saldırı simülatörü, birçok saldırı türünü simüle edebilecek bir altyapı sağlayacak şekilde yapılandırılmıştır. Daha fazla saldırı simülasyonu, gelecekteki tehditlere karşı daha etkili önlem alınmasına neden olacaktır ve atakları daha kısa sürede tespit etme olasılığı ortaya çıkmaktadır. Bu saldırılara ait yapılandırma girişi, simülatör açıldığında yapılandırma formları kullanılarak yüklenmektedir.

Geliştirilen saldırı simülasyon modelinin uygulama aşamaları Şekil 1'de gösterilmiştir. Saldırı modellerinin çalıştırılacağı bir ağ modeli oluşturulmuştur. Gerekli ağ yapısı için bir ağ topolojisi üreteci kullanılmıştır. Bu kapsamda, Şekil 2.'de kavramsal modelde görüldüğü gibi DEVS tabanlı dağıtık büyük ölçekli ağ simülasyon modeline saldırı modelleri entegre edilmiştir.

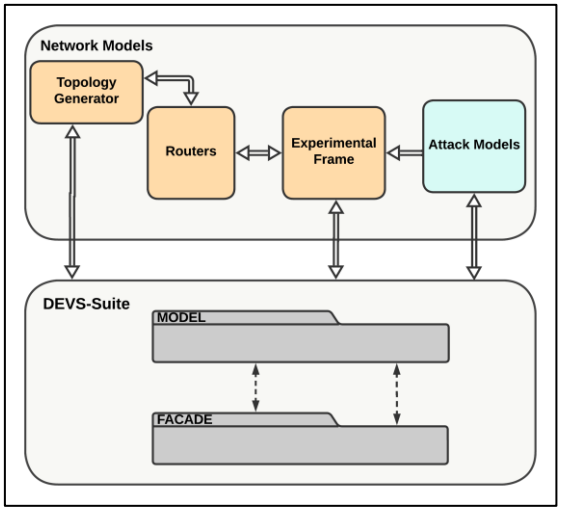
4.1. DoS Saldırıları

Bir DoS saldırısının temel amacı, ağ bağlantılı bir hizmeti aşırı yükleyerek kullanılamaz hale getirmektir. Servis sağlayıcıya gönderilen bu kadar çok sayıda kötü niyetli istek, sunucuyu bir noktadan sonra yanıt veremez

duruma getirir [39]. DoS saldırılarının hedefi genellikle finans kurumları olduğu için hizmet kesintisi, ilgili ağ sistemine zarar vermenin yanı sıra önemli mali kayıplara da neden olabilmektedir [40]. Günümüzde DoS saldırılarını önlemek için pek çok yazılım ve donanım çözümleri geliştirmesine rağmen güvenlik zafiyetleri bulunan cihaz veya web siteleri DoS saldırılarından etkilenmektedirler [41]. Bunun sebeplerinin başında güncellenmemiş ağ cihazları, tecrübesiz güvenlik veya IT çalışanları ve yanlış güvenlik politikaları olarak görülebilir.



Şekil 1. Siber saldırı modelleme aşamaları ve bileşenleri.



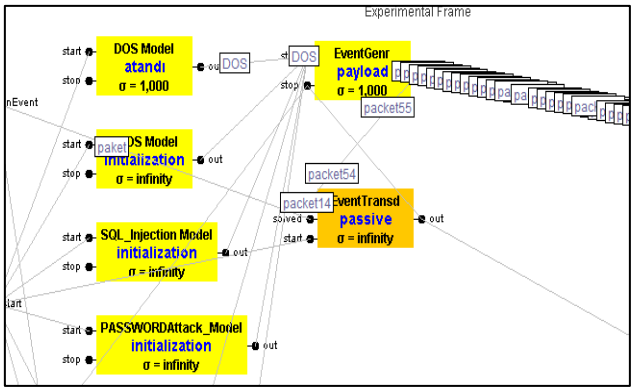
Şekil 2. Kavramsal modeler.

DoS saldırısı ayarlarının yapıldığı formda kurban bilgisayarın ve saldırıyı gerçekleştirecek bilgisayarın IP numaraları ile saldırı kodu ve her adımda gönderilecek paket sayısı bilgisi ayarlanmaktadır. Bu verilerlerle simüle edilen DoS saldırı modeli tetiklenmiş olur. Deneysel çerçevedeki olay üreteci atomik modelinde olaylar otomatik olarak veya giriş bağlantı noktalarına manuel olarak bir giriş olayı oluşturulabilir. Bir girdi olayı, bir bağlantı noktası adını (port adı), veri değerini (paket) ve geçen süreyi içerir. Geçen zaman, ilişkili olayın bir zaman damgasıdır ve belirli bir olayı belirli bir sonlu, gelecek zaman örneğinde planlamak ve enjekte etmek için kullanılır. Geçen zaman, simülatör saati ile ilişkili zaman birimleri cinsinden sağlanır.

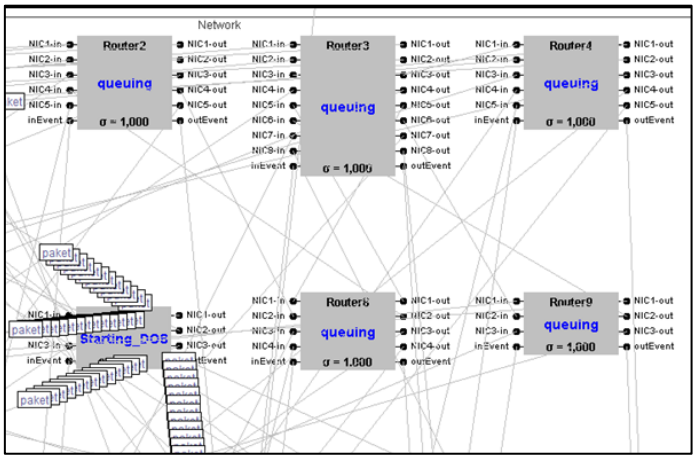
Bütün saldırı modelleri gibi DoS saldırı modelinin çıkışları da Şekil 3.'teki deneysel çerçeve bağlantı görünümü gösterildiği gibi olay üreteci (event generator) atomik modelinin giriş bağlantı noktasına bağlanarak giriş olayı otomatik oluşturulmuştur. Her adımda saldırgan olan cihazın çıkış portlarından hedefi kurban bilgisayar olan ve sayısı saldırı başlangıcında ayarlanan paketler gönderilir.

Geliştirilen uygulamaların test edilmesi için Kanada Siber Güvenlik Enstitüsü (CIC) tarafından paylaşılan CSE-CIC-IDS2018 veri seti kullanılmıştır. Saldırı paketleri oluşturulurken paketlere eklenen saldırı kodları aracılığıyla saldırgan bilgisayarın durumu Şekil 4.'te görüldüğü gibi Starting_DOS olarak değişmekte böylece saldırgan cihaz simülasyon ortamında gözlemlenebilmektedir.

DoS saldırısını başlatan düğümde oluşturulan ve çıkış portlarından gönderilen paketler Şekil 4.'te görüldüğü üzere yoğun bir paket çıkışı şeklinde görülebilmektedir. İlk DoS saldırı uyarısı yapıldığı zaman cihaz tamamen



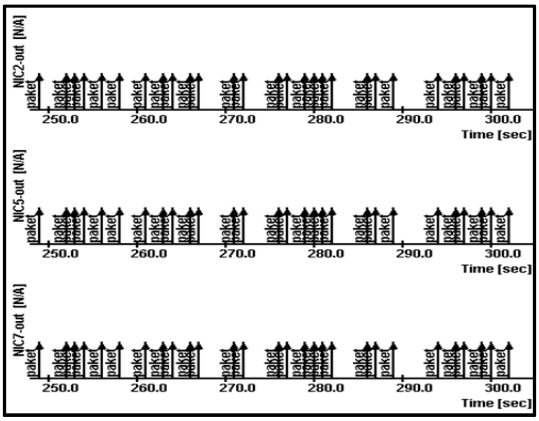
Şekil 3. Deneysel çerçeve bağlantı görünümü.



Şekil 4. Saldırgan bilgisayardan hedefe yönelik saldırı görüntüsü.

servis dışı kaldığı anlamına gelmez, saldırı devam ettiği süre içerisinde hedefe ulaşan paket sayısına bağlı olarak bu uyarı belirli aralıklarla tekrar etmektedir.

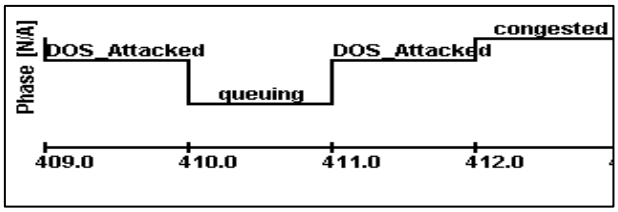
Şekil 5.'te kayıt izleme penceresinden de saldırıyı başlatan cihazın çıkış portlarında görülen paket yoğunluğu zamana bağlı bir grafik ile izlenebilmektedir. Saldırı devam ettirildikten belli bir süre sonra saldırı kesilmezse tamamen tıkanma gerçekleşecek ve Şekil 6.'da grafikten anlaşıldığı üzere kırmızı seviye olan "congested" durumuna geçilecektir ve servis engellenmiş olacaktır.



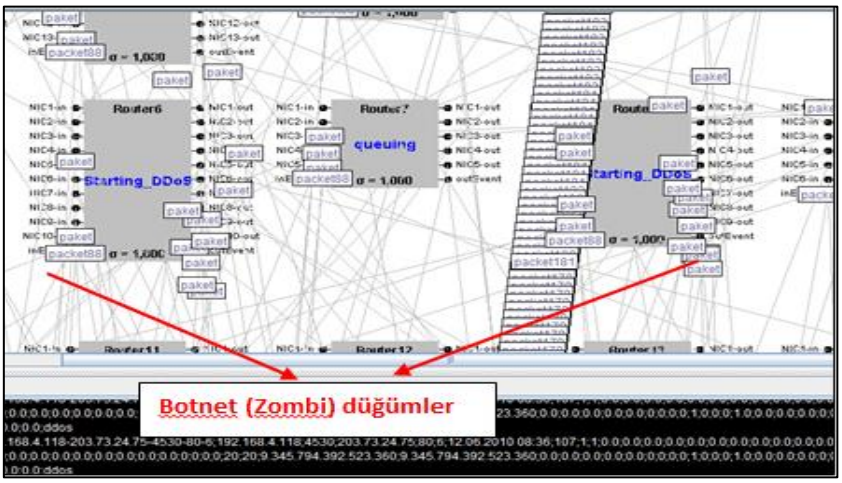
Şekil 5. Çıkış portları izleme penceresi.

4.2. DDoS Saldırısı

DDoS saldırısı, en az bir hedefe karşı bir DoS saldırısı başlatmak amacıyla birçok bilgisayarın kullanıldığı koordineli bir DoS saldırısıdır. Saldırgan, birden fazla bilgisayarın farkında olmadan kaynaklarını kullanarak saldırı başlatır. İstemci/sunucu teknolojisi kullanılırsa artırabilir. Bir DDoS saldırısı, saldırıyı başlatan gerçek saldırgan, zombi bilgisayarları kontrol edebilen güvenliği istismar edilmiş ana bilgisayarlar, zombi bilgisayarlar ve hedef bilgisayar olmak üzere dört kısımdan oluşmaktadır.

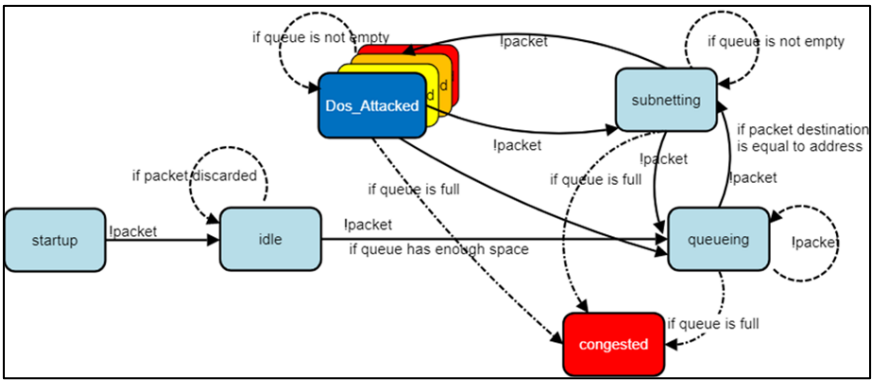


Şekil 6. DoS saldırısı durum geçiş grafiği.



Şekil 7. DDoS saldırı aşamasındaki Botnetler.

Saldırı paketleri oluşturulurken paketlere eklenen saldırı kodları aracılığıyla saldırgan bilgisayarların durumu Şekil 7.'de görüldüğü gibi "Starting_DDoS" olarak değişmekte ve gözlemlenebilmektedir.

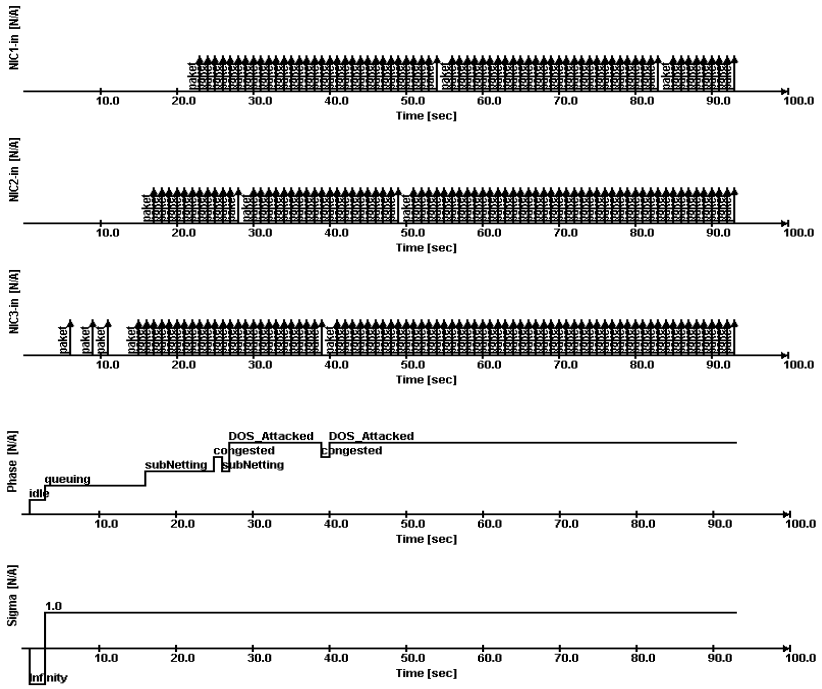


Şekil 8. Hizmet reddi saldırısında hedef düğüm durumları, durum geçişleri.

Bu çalışmada simüle edilen DDoS saldırı modeli başlangıçta belirli parametre verileriyle yapılandırılır. Bu veriler deneysel çerçevedeki jeneratör atomik modelinin giriş portlarına otomatik olarak bir giriş olayı oluşturmaktadır. Bir girdi olayı, bir bağlantı noktası adını (port adı), veri değerini (paket) ve geçen süreyi içerir. DEVS-Suite siber saldırı uygulaması (DEVS-CAS), DEVS-Suite çekirdeğinin üzerine inşa edilmiştir. Düğümler tarafından işlenen olaylar, Şekil 7.'de gösterildiği gibi durum diyagramları şeklinde tanımlanabilir. Sistemdeki olaylar, seçilen saldırı tipine göre seçilir. Saldırı mantığını anlamak için yeterli sayıda vaka kullanılır. Şekil 8.'de DoS ve DDoS saldırılarına ait saldırı altındaki düğümün durum geçişlerini göstermektedir

Simülasyondaki saldırgan ve kurban düğümlerin durumlarını ve çıktıların değişimini görmek ve değerlendirmek için uygulama penceresi kontrol bölümündeki panel yardımıyla saldırı sürdürülür. Her adımda saldırgan olan cihazın çıkış portlarından, hedefi kurban bilgisayar olan ve sayısı saldırı başlangıcında ayarlanan paketler gönderilir. Saldırı emri alan botnetler hedefe yönelik yoğun bir paket trafiği başlatmaktadır. Her adımda üretilecek/gönderilecek paket sayısı saldırı başlamadan önce parametre ayarlarının yapıldığı formda belirtilmektedir. Hedef düğüm yoğun paket akışına hedef oluğunu, düğüme gelen paket sayısı belli bir sayıyı geçtiğinde bunu "DoS_Attacked" durumuna geçerek göstermektedir. Hedef makinanın tampon alanı kısa sürede dolacaktır. Saldırı devam ettiği müddetçe tıkanıklığı sürecektir ve bu cihaz servis dışı kalmaktadır, böylece DDoS saldırısı amacına ulaşmış olacaktır.

Ağ trafiği normal akışını sürdürürken saldırı başladıktan yaklaşık 20 saniye sonra hedef bilgisayarın giriş portlarında sıra dışı bir paket yoğunluğu oluştuğu görülmektedir. Hedef düğüm, giriş portlarındaki yoğun paket

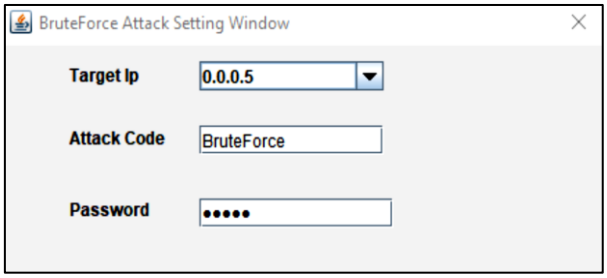


Şekil 9. DDoS saldırısına ait hedef düğümün giriş portlarının durumu ve dururum değişim grafiği.

akışına hedef oluğunu, düğüme gelen paket sayısı belli bir sayıyı geçtiğinde "DoS_Attacket" durumuna geçtiği Şekil 9.'daki grafikte görülmektedir. Hedef makinanın tampon alanı kısa sürede dolmakta ve tıkanma durumuna(congested) geçtiği görülmektedir. Saldırı devam ettiği bu cihaz servis dışı kalmaktadır ve bu DDoS saldırısı amacına ulaşmış olduğunu göstermektedir.

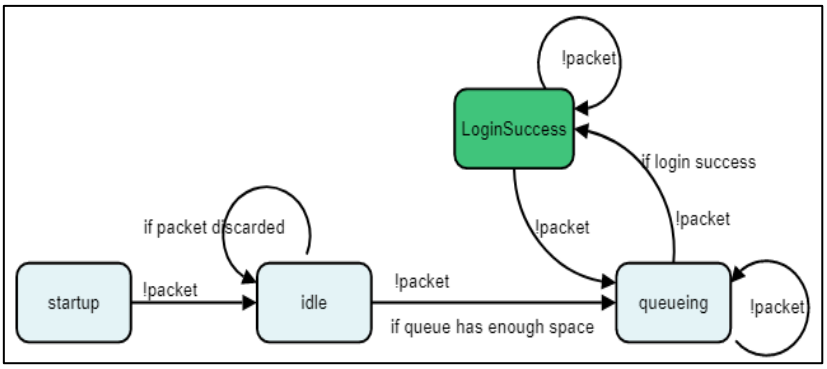
4.3. Kaba Kuvvet Saldırısı

Kaba kuvvet saldırısında saldırganlar, kimlik bilgilerini kırmaya çalışırken, bir şifreyi tahmin etmek için olası her sayı, harf ve karakter kombinasyonunu deneyen bir uygulama veya komut dosyası başlatılır. Bazı durumlarda, başarı şansını artırmak için yaygın olarak kullanılan kimlik bilgilerinin veya sızdırılmış kimlik bilgilerinin listeleri kullanılabilir.
BruteForce yapılandırma penceresinde hedef bilgisayarın IP numarası ve saldırı kodu ile birlikte hedef bilgisayarın oturum açma şifresi Şekil 10.'daki pencereden girilebilmektedir. Şifreyi saldırı simülasyonunda yapılandırma penceresinden belirlemek sadece sistemin doğru sonuç ürettiğini doğrulamak maksadıyladır.

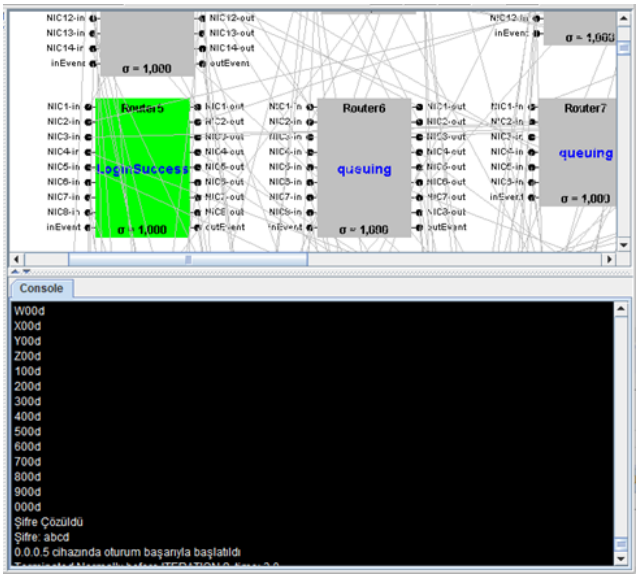


Şekil 10. BruteForce saldırısı yapılandırma penceresi.

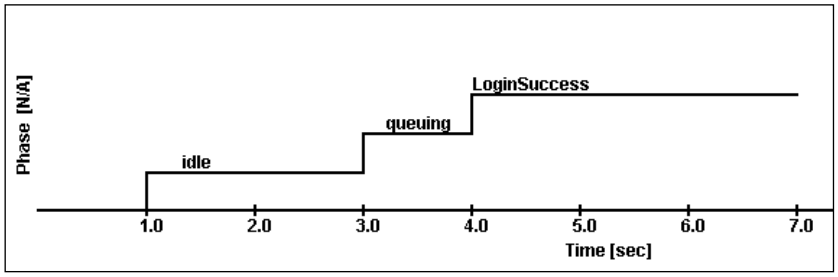
Bu çalışmada kaba kuvvet saldırısını simülasyonunda şifre ihtimallerini denemek için ilgili java sınıfında İngiliz alfabesi büyük ve küçük harfler (a-z, A-Z) ile 0-9 arasındaki sayılar kullanılmıştır. Uzun ve karmaşık şifrelerin bulunması uzun sürmektedir. Özel karakterlerin bulunmadığı bu karakter setinde bile 5 haneli bir şifre için 50 milyondan fazla kombinasyon denemek gerekmektedir. Hedef düğümün durum geçişleri Şekil 11.'de gösterilmiştir.
Hedef düğümde BruteForce nesnesi oluşturulup şifre çözüldükten sonra cihazın durum bilgisi Şekil 12.'deki gibi "LoginSuccess" olarak değişmektedir. Bu da saldırının başarıya ulaştığını gösterecektir. Yapılandırma girişinde seçilecek uzun ve karmaşık bir şifre bu süreyi oldukça uzatacaktır. Sonucu hızlı test edebilmek açısından kısa şifreler kullanmak bekleme süresini azaltacaktır. Hedef düğümün durum değişim grafiği Şekil 13.'te gösterilmiştir.



Şekil 11. Brute Force saldırısında hedef düğüm durumları, durum geçişleri.



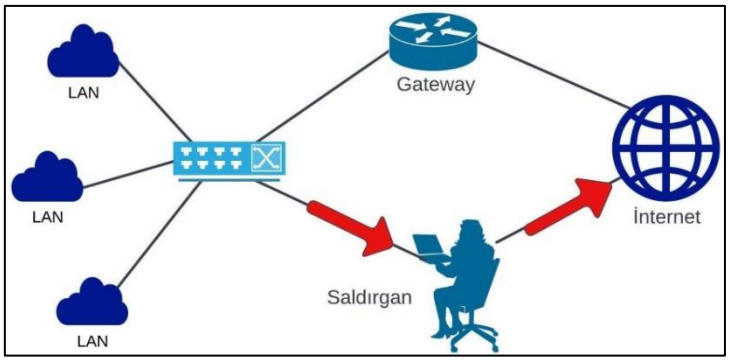
Şekil 12. Brute Force saldırısı başarılı olma durumu.



Şekil 13. Brute Force saldırısında hedef düğüme ait durum değişim grafiği.

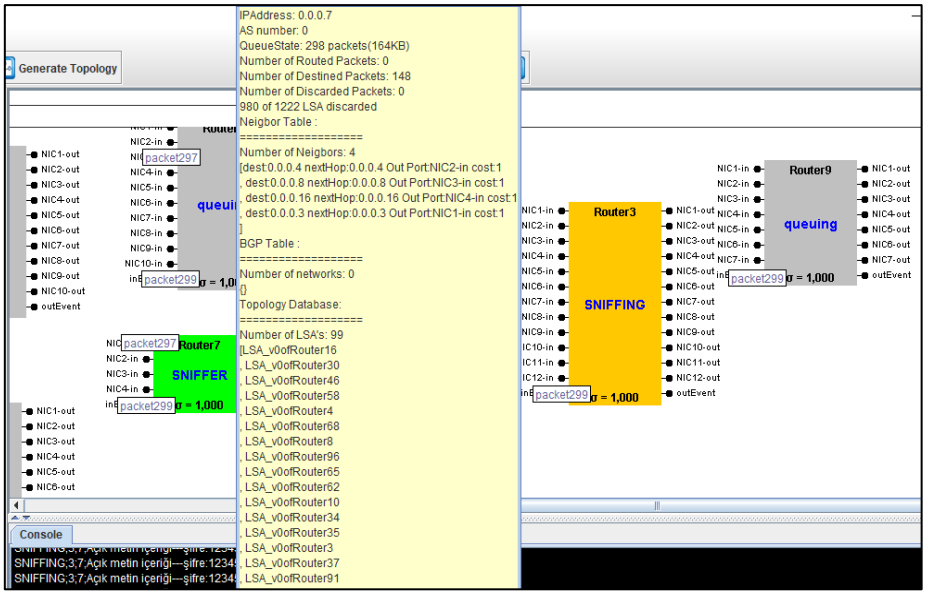
4.4. Paket Koklama Saldırısı

Bilgi güvenliği perspektifinden bakıldığında, paket koklama (sniffing), trafiği yakalanabileceği, analiz edebileceği ve izlenebileceği bir hedefe yönlendirmek anlamına gelmektedir.
Ağ trafiğinin dinlenmesinde temel mantık Şekil 14.'te gösterildiği gibi ağ geçidi cihazına gelen her paket kabul edildiği için iki bilgisayar arasındaki tüm verilerin yakalanarak saklanması olarak tanımlanabilir. Düz metin olarak bilgi içeren herhangi bir ağ paketi, saldırganlar tarafından ele geçirilebilir ve okunabilir. Bu bilgiler, kullanıcı adları, şifreler, gizli kodlar, bankacılık detayları veya saldırgan için değerli olan herhangi bir bilgi olabilir. Bilgisayarlar arasındaki bağlantıların şifreli olması bu saldırıya karşı alınabilecek en önemli önlemdir. Şifreli paketler yakalanabilse bile içeriği anlaşılmayacaktır. Şifreleme algoritmasının da saldırılara karşı dayanıklı ve uygun performans sağlayan yapıda olmalıdır. Genel olarak pasif ve aktif olarak nitelenen iki koklama türü vardır. Koklama yapan cihazın ağ kartının "promiscius" modda çalışması sağlanmalıdır. Böylece portlarına gelen her paketi kabul edebilecektir. Saldırgan düğüm tüm paketleri yani farklı IP adreslerine sahip paketleri de kabul edecek şekilde yapılandırılabilmektedir. Şekil 15.'deki örnekte test amacıyla sadece belirli bir hedef düğüm dinlenmiştir.



Şekil 14. Ağ trafiğinin dinlenmesi.

Simülatörde koklama saldırı modelini çalıştırdığımızda bir süre sonra koklama yapılan düğümün durumu "SNIFFING" olarak değişmektedir, saldırgan konumundaki paket koklayıcı düğümün durumu "SNIFFER" olarak izlenebilmektedir ve fare işaretçisini düğümün üzerine getirdiğimizde anlık istatistik listesi görülmektedir. Bu listede bu düğüme o ana kadar gelen paket sayısı görülmektedir. Test amacıyla hedef düğüme gönderilen paketlerin içerisinde şifrelenmemiş açık metin içeriğine örnek olacak bir metin yerleştirilmiştir. Dinlenen düğümden elde edilen paketlerin içeriği okunarak konsol penceresinde yazdırılmıştır ve konsolda pakette bulunan saklı metin görülebilmektedir. Paket koklayıcılar ancak açık metinleri okuyabilirler, şifrelenmiş mesajlar yakalansa bile içeriği okunamaz kabul edilmektedir.



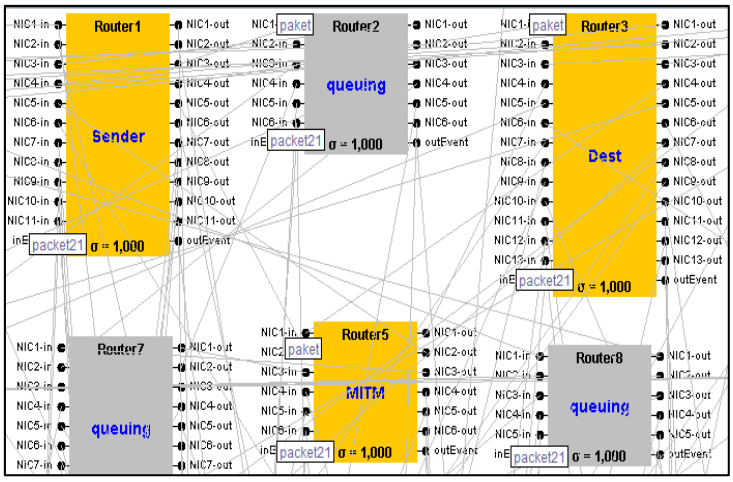
Şekil 15. Paket koklayıcı cihazın durumu ve paket istatistiği.

4.5. Ortadaki Adam Saldırısı

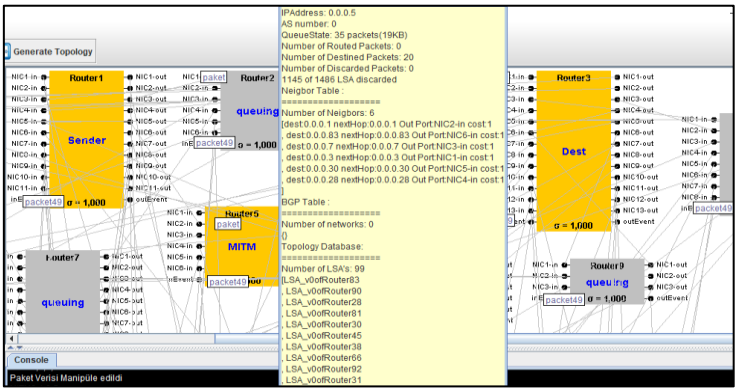
Ortadaki adam (MITM) saldırısında, saldırgan iki hedef arasındaki iletişimi gizlice dinler ve ardından birbirleriyle doğrudan iletişim kurduklarına inanan iki taraf arasındaki mesajları gizlice aktarır veya değiştirir. Ortadaki adam saldırılarının bir örneği, saldırganın kurbanlarla bağımsız ilişkiler kurduğu ve kurbanların birbirleriyle özel bir ilişki üzerinden doğrudan konuştuklarına güvenmelerini sağlamak için aralarında mesajlar aktardığı dinamik gizli dinlemedir. Tüm iletişim saldırgan tarafından kontrol edilir. Saldırgan, iki taraf arasında geçen her önemli mesajı engelleme ve yenilerini enjekte etme kapasitesine sahip olmalıdır.

Araya girilerek dinlenecek kurban seçilen cihazlar ile saldırgan düğümün IP numarası saldırı yapılandırma ara yüzünde tanımlanmaktadır. Saldırı kodları her saldırı için saldırı imzası niteliğindedir, atomik düğümlerde saldırılara ait durum geçişleri bu saldırı kodları kullanılarak yapılmaktadır. Simülasyon başladığında iletişimde olan kurban düğümlerden olan mesaj gönderen kaynak düğümün durumu "Sender", mesajı alan hedefin durumu "Dest" ve araya girip paketleri üzerinden geçiren saldırgan düğümün durumu "MITM" olarak Şekil 16.'da gösterilmektedir.

Kurban olarak seçilen cihazlar arasındaki bütün paket trafiği araya girip paketleri almak suretiyle dinlenmektedir. Bu duruma ait istatistikler ve elde edilen paketlere ait port izleme ekranı görüntüsü Şekil 19.'da görülmektedir. Saldırgan durumundaki düğümün üzerine fare işaretçisi odaklandığı zaman görünen yardımcı ileti penceresinden süzülen paket miktarı ve kuyrukta bekleyen paketler Şekil 17.'de görülmektedir.

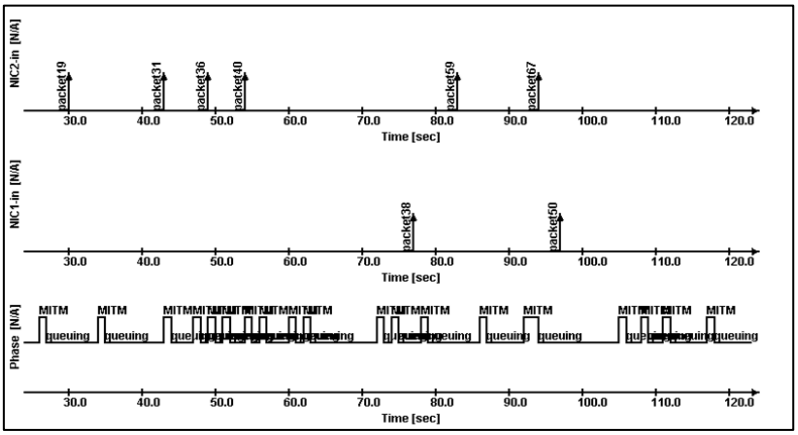


Şekil 16. Hedef, kaynak ve saldırgan düğümlerin durumu.



Şekil 17. Araya girip dinleme yapan düğümün durumu ve verileri.

Saldırgan düğüm yakaladığı paketleri istediği gibi manipüle ederek alıcı düğüme iletebilmektedir. Bu testi doğrulamak için pakete "Paket verisi manipüle edildi" datası eklenerek konsol penceresinde paket içeriğindeki mesaj gösterilmiştir. Ortadaki adam saldırısına ait paket ve durum değişim grafikleri Şekil 18.'de gösterilmiştir.

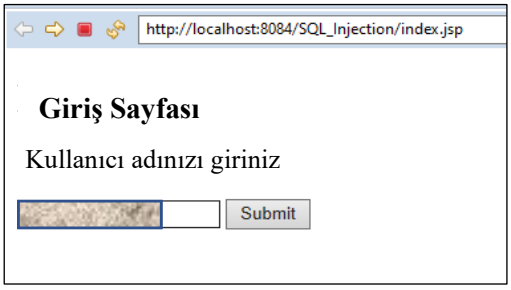


Şekil 18. Ortadaki adam saldırısına ait paket ve durum değişim grafikleri.

4.6. SQL Enjeksiyonu (SQL Injection)

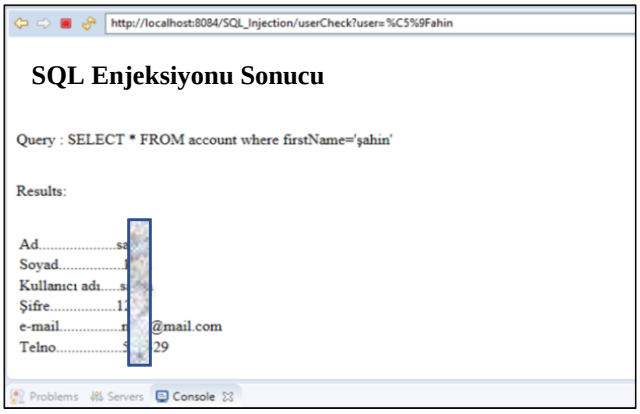
SQL, bir veri tabanına bağlanmak ve iletişim kurmak için kullanılır. İlişkisel veri tabanı yönetim sistemleri için standart dildir. SQL sorguları, veri girişi, güncellemeler ve kayıt silme gibi komutları yürütmek için kullanılır. SQLI olarak da bilinen SQL enjeksiyonu, görüntülenmesi amaçlanmayan bilgilere erişmek için veri tabanına yönelik bir saldırı türüdür. Bu bilgiler, kişisel veriler, hassas şirket verileri, müşteri bilgileri veya kullanıcı listeleri dahil olmak üzere pek çok öğeyi içerebilir. SQLI, web uygulamalarından elde edilen kullanıcı girdileri ile oluşturulan SQL sorgularının kötü niyetle kullanmak olarak da tanımlanabilir [42SQL enjeksiyonunun bir kurum veya organizasyona yönelik etkisi geniş kapsamlıdır. Başarılı bir SQL enjeksiyonu saldırısı, kullanıcı verilerinin izinsiz görüntülenmesine, saldırganın bir veri tabanında yönetici yetkilerini kazanmasına ve tüm tabloların silinmesine sebep olabilir ve bunların tümü bir işletmeye büyük zarar verir.Bu çalışmada, bir Java

teknolojisi olan Jsp- MySql tabanlı bir web uygulamasına yönelik, bir SQL enjeksiyonu saldırısı ve analizi gösterilmiştir.



Şekil 19. Login sayfası.

Sql sorgularının manipülasyonunu göstermek için login sayfas olan index.jsp basit tutulmuştur. Şekil 19.'da "Giriş Sayfası" sayfasından girilen kullanıcı adına göre önceden Mysql Workbench ile hazırladığımız veritabanına erişebilmek için gerekli sürücüler çalıştırılıp bağlantı kurulduktan sonra bu kullanıcıya ait kayıt varsa Şekil 20.'deki "SQL Enjeksiyonu Sonucu" sayfasında listelenecektir.

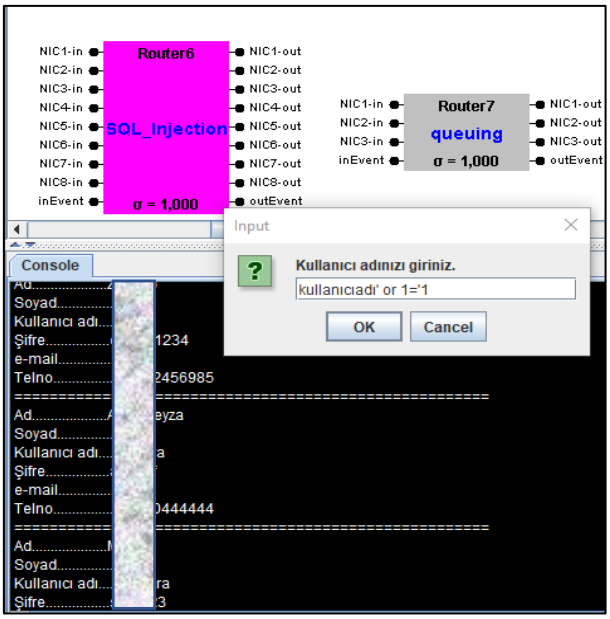


Şekil 20. SQL sorgu sonucu.

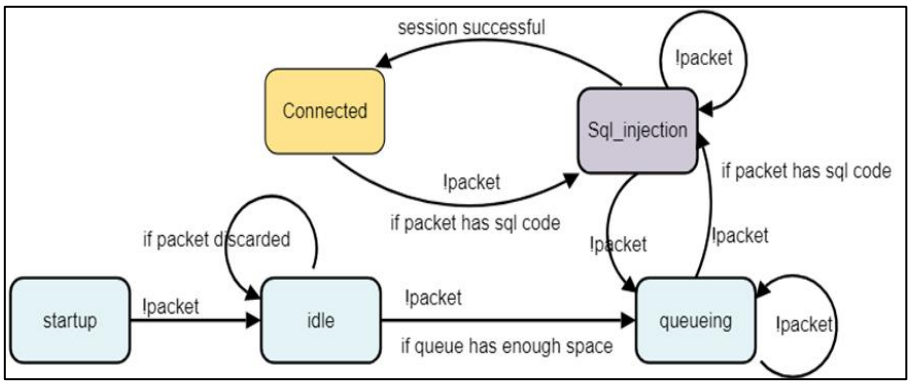
Burada sorgulama kullanıcı adına göre yapılmakta ve sadece girilen kullanıcı adına ait kayıt listelenmektedir. Yukarıda yapılan işlemler normal kullanıcı davranışıdır ve nizami kullanıcı girişi yapılmaktadır .
Jsp-MySQL tabanlı web uygulaması üzerinde saldırı örneği ve analizi sunulan SQL enjeksiyonu saldırısını DEVS-CAS saldırı simülatöründe gerçekleştirmek için ilgili saldırı modelinin yapılandırma penceresi kullanarak saldırı başlatılır. Kullanıcı adı girişi Şekil 21.'deki gibi yaparken kullanıcı adı yerine basit bir SQL enjeksiyonu ifadesi yazıyoruz. Bu yazılan ifade sorguyu manipüle edecektir ve bütün kullanıcılara ait kayıtları listeleyecektir. SQL enjeksiyonunu yürütmek isteyen bir saldırgan, bir veritabanındaki doğrulanmamış giriş güvenlik açıklarından yararlanmak için standart bir SQL sorgusunu manipüle eder. SQL enjeksiyonu ifadesi girilip çalıştırıldığında veritabanında bulunan bütün kullanıcılara ait kayıtlar listelenmektedir. SQL enjeksiyonu yöntemleri çoktur, burada sadece basit bir yöntem gösterilmiştir.
SQLI saldırı simülasyonu başlangıcında hedef düğüme gelen paketin adresi doğrulandıktan sonra paket içeriğinde SQL sorgusu varsa düğüm "Sql_injection" durumuna geçmektedir. SQL enjeksiyonu sonucunda hedef düğümde veritabanına bağlantı yapılıp başarılı bir oturum gerçekleşirse düğüm "connected" durumuna geçmektedir. Hedef düğümün durum geçişleri Şekil 22.'de ve durum değişim grafiği Şekil 23.'de gösterilmiştir.

5. SİMÜLASYON DENEY SONUÇLARI

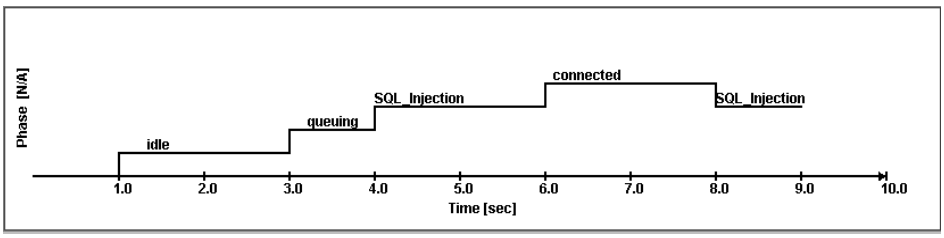
Bu bölümde saldırı hedefindeki cihazda gerçekleşen olaylar, durum değişimleri, saldırı uyarıları ve portlarındaki trafik yoğunluğu grafiksel olarak gösterilerek elde edilen sonuçlara göre saldırının başarımı değerlendirilmiştir. Saldırı uygulama bölümünde belirli saldırılara ait deney çıktıları gösterilmiştir, deney çıktıları verilmeyen DoS ve DDoS saldırılarına ait deney çıktıları bu bölümde gösterilecektir.
Ağ simülasyonu bir DoS saldırısı ile başlasa bile ağ trafiği belirli bir yoğunluğa kadar bir süre normal şekilde işlemeye devam edecektir. Normal ağ trafiği devam ederken ve hizmet reddi saldırısı olmadığında bile düğüm tıkanıklığı oluşabilir. Ancak bu, bunun bir DoS saldırısı olduğu anlamına gelmez. Belirli bir düğüme ulaşan paketler incelendiğinde, aynı kaynaktan gelen paketlerin fark edilebileceği şekilde yapılandırılır. Aynı kaynaktan gelen paket sayısı belirli bir değeri aştığında anormal bir durum olduğuna karar verilir ve DoS saldırı uyarısı verilir. Zamana bağlı olarak artan paket sayısına göre farklı güvenlik risk seviyeleri Şekil 24.'te belirlenmiştir.



Şekil 21. SQL enjeksiyonu sonucu elde edilen kayıtlar.



Şekil 22. SQLI saldırısında hedef düğüm durumları, durum geçişleri.



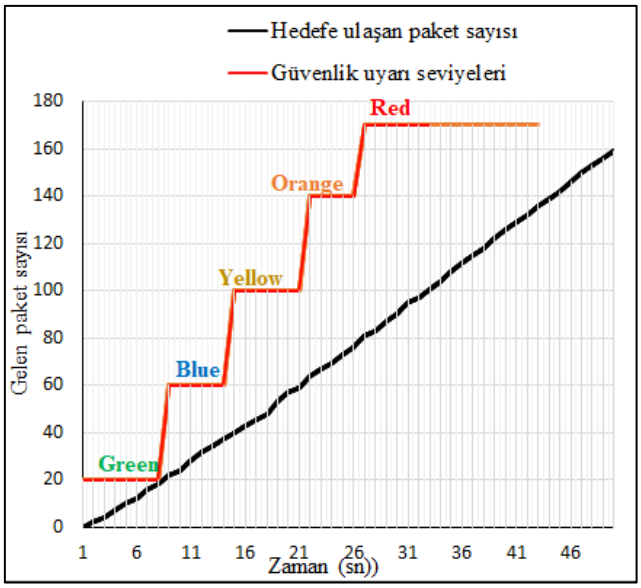
Şekil 23. SQLI saldırısında hedef düğüme ait durum değişim grafiği.

Simülasyon ortamındaki hedef cihazın rengi de grafikteki renklere göre renk değiştirmektedir. Bu da tehlikeyi fark etmek için gözlemciye kolaylık sağlamaktadır.

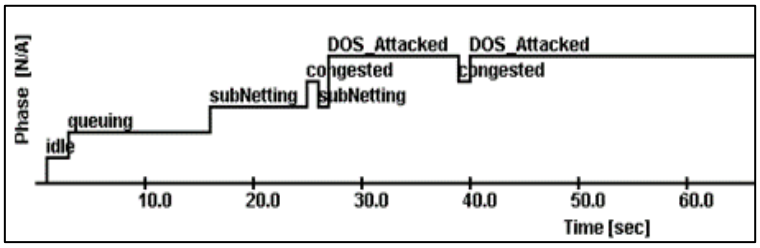
Belirli bir kaynaktan gönderilen paketler, belirli bir sayıya kadar herhangi bir anormalliğe neden olmaz. Bu durum yeşil seviye olarak gösterilmiştir. Atomik model konfigürasyonunda normal ağ trafiği olarak kabul edilebilir seviye için simülasyon süresi ile 10 saniyede 20 paket olarak konfigüre edilmiştir. Bu seviye aşıldıktan sonra anormal durum olarak kabul edilir ve bu anormal duruma göre DoS saldırı uyarı alarmı verilir

DDoS saldırıları, DoS saldırılarının bir alt sınıfıdır. Bir DDoS saldırısı, toplu olarak botnet olarak bilinen ve sahte trafikle hedef düğümü hizmet veremez duruma getirmek için kullanılan birden çok cihazı içerir. Saldırı emri alan botnetler hedefe yönelik yoğun bir paket trafiği başlatmaktadır. Hedef düğüm yoğun paket akışına hedef olduğunu, düğüme gelen paket sayısı belli bir sayıyı geçtiğinde bunu DoS_Attacked durumuna geçerek göstermektedir. Hedef makinanın tampon alanı kısa sürede dolacaktır. Saldırı devam ettiği müddetçe tıkanıklığı sürecektir ve bu cihaz servis dışı kalmaktadır, böylece DDoS saldırısı amacına ulaşmaktadır.

DoS saldırıları uyarı seviyeleri DDoS için de geçerlidir. Şekil 25.'te hedef düğümde saldırıya ait grafiksel gösterimler görülmektedir. Ağ trafiği normal akışını sürdürürken saldırı başladıktan yaklaşık 20 saniye sonra hedef bilgisayarın giriş portlarında sıra dışı bir paket yoğunluğu oluştuğu görülmektedir. Hedef düğüm yoğun paket akışına hedef oluğunu, düğüme gelen paket sayısı belli bir sayıyı geçtiğinde bunu "DoS_Attacked" durumuna geçerek göstermektedir. Hedef makinanın tampon alanı kısa sürede dolmakta ve tıkanma (congested)



Şekil 24. Güvenlik uyarı seviyeleri.

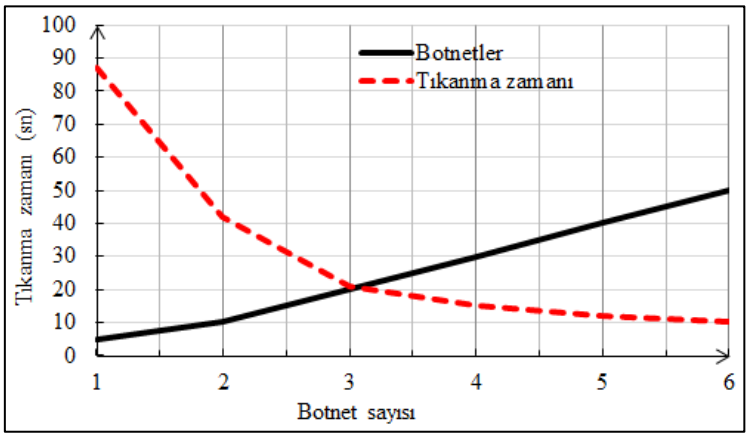


Şekil 25. DDoS saldırısına ait hedef düğüm durum geçiş grafiği.

durumuna geçtiği görülmektedir. Saldırı devam ettiği müddetçe tıkanıklığı sürmektedir ve bu cihaz servis dışı kalmaktadır ve DDoS saldırısı amacına ulaşmıştır.

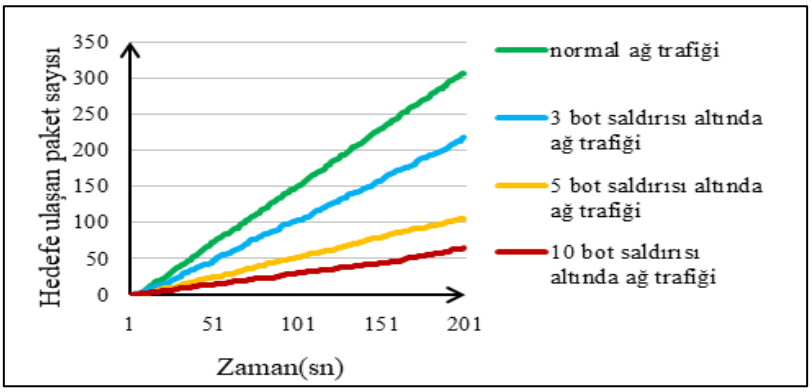
Botnetlerin kullanıldığı bir DDoS saldırısının etkileri bot sayısına bağlı olarak değişmektedir. Bir hizmet reddi saldırısının temel amacı tıkanıklık oluşturup sunucuyu servis veremez duruma getirmek olduğu için aynı anda ne kadar çok istek gönderilirse tıkanma o kadar çabuk gerçekleşir. DDoS saldırılarının başarılı olabilmesi için olabildiğince farklı kaynaklardan hedefe mesaj/paket isteği göndermek gerekir. Botnetler daha çok bu amaçla kullanılmaktadır. Saldırıda kullanılan bot sayısı arttıkça tıkanma süresi kısalacaktır. Bu durum, simülasyon sonucunda elde edilen verilerle Şekil 26.'deki grafikle gösterilmiştir. Grafikten botnet sayısı ile tıkanma süreleri arasında bir ters orantı olduğu görülebilmektedir. Şekil 25.'de 100 düğümlü bir ağda değişen sayıdaki zombi içeren botnetler ile yapılan DDoS saldırısında hedef düğümde bot sayısına bağlı olarak tıkanmanın gerçekleştiği zaman grafiği gösterilmektedir.

Bot sayısındaki artışla orantılı olarak tıkanma süresi kısalmaktadır ve bu olması beklenen durum grafikten de anlaşılmaktadır. Saldırı simülasyonunda bot sayısı teorik olarak ağdaki düğüm sayısından az olmalıdır.



Şekil 26. Botnet sayısına dayalı tıkanıklık grafiği.

Bu kurala bağlı kalarak ağdaki bot sayısı adımadım arttırılarak benzetimi yapılan ağda ağ trafiğinin nasıl etkilendiği gözlemlenmiştir. Normal ağ trafiğinin DDoS saldırısından nasıl etkilendiğini göstermek için belli sayıdaki botnetlerle yapılan saldırıda elde edilen trafik verileri ile normal trafik verileri Şekil 27.'da birlikte gösterilmiştir. Grafikte görüldüğü üzere sabit bir ağdaki botnetlerin sayısı arttırıldıkça ağ trafiği orantılı olarak yavaşlamaktadır. Ağ trafiği hedefe ulaşan paket sayıları ile orantılı olarak gösterilmiştir.



Şekil 27. Farklı bot sayıları ile DDoS saldırısı altında ağ trafiği grafiği.

6. SONUÇ

Bir kurumsal ağı fiziksel olarak gerçekleştirmek ve bu ağlarda yeni siber güvenlik yöntemlerini test etmek maliyetlidir ve test verilerinin elde edilmesi de çok zaman alıcıdır. Kurumsal ağ tasarımı aşamasında ise güvenilir bir simülasyon aracı ile ağ tasarımının oluşturulması, güvenlik simülasyonlarının yapılması ve ağ tasarımlarının doğrulanması maliyet ve zaman tasarrufu sağlamaktadır. Bu çalışmada geliştirilen siber saldırı simülatörü, simülasyon ortamında tasarlanan ağdaki belirli siber saldırılara ilişkin uyarı verilerinin verimli bir şekilde elde edilmesi için bir araç sunmaktadır. Bu araç belirli saldırı türleri için uyarı verileri elde etmek için kullanılsa da, daha farklı saldırı türleri için uyarı verileri oluşturmak için genişletilebilir bir altyapı sağlar. Geliştirilen uygulama, simüle edilen ağ üzerinde saldırı modelleri çalıştırabilme ve sonuçlarını izleyebilme özelliğine sahiptir. Bu çalışmada, büyük ölçekli kurumsal ağların kolaylıkla tasarlanabileceği ve geçerli düzeyde performans, ölçeklenebilirlik ve doğruluk ile siber güvenlik testlerinin kısa sürede yapılabileceği görülmüştür. Uygulama, ağ benzetiminin oluşturulmasına izin veren ağ modelleme yetenekleri ile ayrıntılı saldırı senaryoları oluşturmak ve benzetimi yapılan ağ modeli üzerinde saldırı eylemlerini simüle etmek için kullanılan saldırı modelleme yetenekleri sağlar. DEVS-CAS ek olarak saldırı eylemleri ile ilişkili ağ trafiğinin modellenmesini, saldırıların algılanması ve uygun saldırı uyarılarının üretilmesini içermekltedir. Ağ modelinin işlevselliği ve saldırı simülasyonu, bazı farklı yaklaşımlarla doğrulanır. Saldırı uyarılarının üretimi, simüle edilen belirli saldırı eylemlerine karşı saldırı hedefindeki cihaz log çıktıları kontrol edilerek doğrulanır. Bu çalışmada geliştirilen DEVS-CAS çerçevesi, hem modellenmiş bir ağ üzerinden saldırıların ilerlemesini hem de bu tür saldırılar sonucunda doğru IDS uyarılarının oluşturulmasını başarılı bir şekilde simüle etmektedir. Ağ modelleri ve saldırı senaryoları çok detaylı bir şekilde oluşturulabilir ve kontrol edilebilir. Ek olarak, saldırı senaryoları kolayca çalıştırılabilir ve değiştirilebilir.

Çalışmaların çoğunda olduğu gibi, bu çalışmanın sonuçlarının elde edilmesi de sınırlamalara tabidir. Elde edilen sonuçlar bu sınırlamalar ışığında değerlendirilmelidir. Gerçekleştirilen siber saldırı modelinin testleri ortalamanın üzerinde bir konfigürasyona sahip kişisel bir bilgisayarda yapılmıştır. Sınırlı işlemci ve bellek kaynakları, benzetimi yapılan sanal ağın düğüm sayısını da sınırlamıştır. Uygulamanın geliştirildiği DEVS-Suite yazılımı ile ayrık olay modellerinin paralel ve dağıtılmış simülasyonu gerçeklitirilebilmektedir. Gelecekteki araştırmalarda bu uygulama dağıtık ve parallel işlem yapan bilgisayar kümelerinde çalıştırılarak bu sınırlama aşılabilecektir ve çok büyük ölçekteki ağlarda da siber saldırı benzetimleri kolaylıkla yapılabilecektir. Bu da elde edilen sonuçlara etkisi olabilecek gerçek fiziksel sistemlerin daha fazla özelliklerinin sanal modellere dahil edilmesini sağlayacaktır.

Artan siber tehditlere karşı sürekli olarak yeni araçlar ve yöntemler geliştirilmektedir. Mevcut siber güvenlik araçlarının ve geliştirilen yöntemlerin test edilmesi için bilimsel araştırmalara ihtiyaç duyulmaktadır. Sanal test ortamlarında test sonuçlarının gerçekliğini artırmak için simülasyon araçlarının yetenekleri detaylı olarak incelenmelidir. Siber güvenlik araştırmalarının daha iyi yapılabilmesi için üniversitelerde siber güvenlik uygulama laboratuvarlarının açılmasının teşvik edilmesi ve eğitim süreçlerine siber güvenliğin eklenmesi ile mümkün olacaktır.

Yazar Katkıları

Şahin Kara- Makale yazımı, literatür araştırması, yöntem, veri işleme, deneysel çalışmalar.
Ahmet Zengin- Özet, yöntem, denetleme ve danışmanlık
Selman Hızal- Literatür araştırması, format düzenleme, sonuç ve çıkarımlar.

Çıkar Çatışması

Makale yazarları aralarında herhangi bir çıkar çatışması olmadığını beyan ederler

KAYNAKÇA

[1] M. Rai, H. Mandoria "A study on cyber crimes cyber criminals and major security breaches", Int. Res. J. Eng. Technol., vol. 6, no. 7, pp. 1-8, 2019.

[2] S. McClure, J. Scambray, G. Kurtz "Network Security Secrets And Solutions", McGraw-Hill Osborne Media, 2005.

[3] F. Cohen "Simulating cyber attacks, defences, and consequences. Computers and Security", vol. 18, no. 6, pp. 479–518, 1999.

[4] S. Park, J-S. Lee, H. K. Kim, J-R. Jeong, D-B.Yeom, S-D Chi "Secusim: A tool for the cyber-attack simulation. Information and Communications Security", Third International Conference on. Springer, pp. 471–475, 2001.

[5] Kotenko, E. Man'kov "Experiments with simulation of attacks against computer networks, International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security", Springer, vol. 2776, pp. 183–194, 2003.

[6] J. Kim, H. Kim, "JDEVS-based modeling methodology for cybersecurity simulations from a security perspective", KSII Transactions on Internet and Information Systems (TIIS), vol. 14, no. 5, pp. 2186-2203, 2020.

[7] E.T. Dougherty, P.G. Gonslaves "Adaptive cyber-attack modeling system. Sensors, and Command, Control, Communications and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense", SPIE, vol. 6201, pp. 16-24, 2006.

[8] S. Cheung, U. Lindqvist, M. W. Fong "Modeling multistep cyber attacks for scenario recognition", IEEE vol. 1, pp. 284-292, 2003.

[9] M. Sudit, A. Stotz, M. Holender, "Situational awareness of a coordinated cyber attack", SPIE, vol. 5812, pp. 114-129, 2005.

[10] G. Ashish, U. Shambhu, R. Chinchani, K. Kevin "SIMS: A Modeling and Simulation Platform for Intrusion Monitoring/Detection Systems", Summer Computer Sımulatıon Conference, pp. 89-94, 2003.

[11] L.L. DeLooze, C. Graig., P. McKean, J.R. Mostow "Incorporating simulation into the computer security classroom", 34th Annual Frontiers in Education. FIE, IEEE, vol. 3, pp. 13-18, 2004.

[12] J. Kistner "Cyber Attack Simulation and Information Fusion Process Refinement Optimization Models for Cyber Security", Masters Thesis, Department of Industrial and Systems Engineering, Rochester Institute of Technology, Kate Gleason College of Engineering, 2006.

[13] Kotenko, A. Ulanov "Agent-based simulation of DDoS attacks and defense mechanisms", Journal of Computing, vol. 4, no. 2, pp. 16–37, 2005.

[14] M.E. Kuhl., M. Sudit "Cyber Attack Modeling and Simulation for Network Security Analysis", IEEE Simulation Conference, pp. 1180–1188, 2007.

[15] B. Van Leeuwen, V. Urias, J. Eldridge, C. Villamarin, R. Olsberg "Performing cyber security analysis using a live, virtual, and constructive (LVC) testbed", Proceedings - IEEE Military Communications Conference MILCOM, pp. 1806–1811, 2010.

[16] G. Torres, K. Smith, J. Buscemi, S. Doshi, H. Duong, D. Xu, H. K. Pickett "Distributed StealthNet (D-SN): Creating a live, virtual, constructive (LVC) environment for simulating cyber-attacks for test and evaluation (T&E)", Proceedings - IEEE Military Communications Conference MILCOM, pp. 1284–1291, 2015.

[17] R. Norman, E.D. Christopher "Cyber Operations Research and Network Analysis (CORONA) Enables Rapidly Reconfigurable Cyberspace Test and Experimentation", Modelıng and Simulation Coordination Office Publication, pp. 15-24, 2013.

[18] Kotenko, A. Chechulin "A Cyber Attack Modeling and Impact Assessment Framework", 5th International Conference on In Cyber Conflict, IEEE, pp. 1–24, 2013.

[19] Ekelhart, E. Kiesling, B. Grill, C. Strauss, C. Stummer "Integrating attacker behavior in IT security analysis: a discrete-event simulation approach", Information Technology and Management, vol. 16, no. 3, pp. 221–233, 2015.

[20] D. Bergin "Cyber-attack and defense simulation framework", Journal of Defense Modeling and Simulation, vol. 2, no. 4, pp. 383–392, 2015.

[21] S. Hansman, R. Hunt "A taxonomy of network and computer attacks, Computers Security", Computers and Security, vol. 24, no. 1, pp. 31–43, 2004.

[22] V.M. Igure, R.D. Williams "Taxonomies of attacks and vulnerabilities in computer systems", IEEE Communications Surveys and Tutorials, vol. 10, no. 1, pp. 6-19, 2008.

[23] J. Friedman, D.V. Hoffman "Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses", Information, Knowledge, Systems Management, vol. 7, no. 1, pp. 159-180, 2008.

[24] C. Myers, S. Powers, D. Faissol "Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches", Lawrence Livermore National Laboratory, vol. 7, pp. 1-22, 2009.

[25] P.K. Singh, A.K. Vatsa., R. Sharma, P. Tyagi "Taxonomy based intrusion attacks and Detection management scheme in peer-to-peer network", International Journal of Network Security and Its Applications (IJNSA), vol. 4, no. 5, pp. 167-179, 2012.

[26] N. Ye, C. Newman, T. Farley "A system-fault-risk framework for cyber attack classification", Information, Knowledge, Systems Management, vol. 5, no. 2, pp. 135- 151, 2006.

[27] Avizienis, J.C. Laprie, B. Randell, C. Landwehr "Basic concepts and taxonomy of dependable and secure computing", Dependable and Secure Computing, IEEE Transactions, vol. 1, no. 1, pp. 11-33, 2004.

[28] Brathen "Correlating IDS alerts with system logs by means of a network-centric SIEM solution", Master's Thesis, Department of Computer Science and Media Technology, Gjovik University, 2011.

[29] M. Collins, C. Gates, G Kataria "A model for opportunistic network exploits: The case of P2P worms." In Workshop on the Economics of Information Security (WEIS), University of Cambridge, 2006.

[30] Dodiya, U.K. Singh "Identification of Taxonomic Features through Assessment of Existing Taxonomies for Vulnerabilities Identification", International Journal of Computer Applications, vol. 174, no. 31, pp. 14–22, 2021.

[31] M. Kjaerland "A taxonomy and comparison of computer security incidents from the commercial and government sectors" Computers and Security, vol. 25, no. 7, pp. 522-538, 2006.

[32] L. Lough "A taxonomy of computer attacks with applications to wireless networks", PhD thesis, Virginia Polytechnic Institute and State University, 2001.

[33] B. K. Mishra, H. Saini, "Cyber attack classification using game theoretic weighted metrics approach", World Applied Sciences Journal, vol .7, pp. 206-215, 2009

[34] P. Monahan, T. Mary "Attack Evolution: Identifying Attack Evolution Characteristics to Predict Future Attacks" PhD Thesis,, Institute of Systems Research University of Maryland, 2006.

[35] K. Nasr, A. El Kalam, A. Fraboul "Generating Representative Attack Test Cases for Evaluating and Testing Wireless Intrusion Detection Systems", International Journal of Network Security and Its Applications (IJNSA), vol. 4, no. 3, pp. 1-19, 2012.

[36] S.R. Nunes "Web attack risk awareness with lessons learned from high interaction honeypots", PhD thesis, Carnegie Mellon University, 2009.

[37] J. Rutkowska "Introducing stealth malware taxonomy", COSEINC Advanced Malware Labs, vol. 1, no.1, pp. 1-9, 2006.

[38] M. Saber, T. Bouchentouf, A. Benazzi, M. Azizi "Amelioration of attack classifications for evaluating and testing intrusion detection system", Journal of Computer Science, vol. 6, no. 7, pp. 716-722, 2010.

[39] America's Cyber Defence Agency, "Understanding Denial-of-Service Attacks" Url:https://www.cisa.gov/uscert/ncas/tips/ST04-015. (Erişim Tarihi: 10.02.2023).

[40] M.F. Hasan, and N.S. Al-Ramadan "Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks" Case. Soc. Sci. Humanit. J, vol. 5, no. 8, pp. 2312-2323, 2021.

[41] F.E. Lubna, D.P. Robert "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges", Future Generation Computer Systems, vol. 122, no. 1, pp. 149-171, 2021.

[42] J. Myllyla, A. Costin "Reducing the Time to Detect Cyber-attacks: Combining At-tack Simulation With Detection Logic", Proceedings of the 29th Conference of Open Inno-vations Association FRUCT, pp. 465-474, 2021.