SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES
VOL. 3, NO. 3, DECEMBER 2020
DOI: 10.35377/saucis.03.03.721364

Analysis of Different Types of Network Attacks on the GNS3 Platform

Resul Daş[1], Burak Bitikçi[2]
[1]Corresponding Author; Fırat University Software Engineering, Elazığ; rdas@firat.edu.tr;
+90 424 237 00 00
[2]Fırat University Software Engineering, Elazığ; burakbitikci@gmail.com;

Received 16 April 2020; Revised 28 September 2020; Accepted 2 November 2020; Published online 30 December 2020

Abstract

In this study, DDoS, SQL injection and XSS attacks that hackers use most in cyber attacks are modeled on GNS3 emulator platform and network security is analyzed. A network scenario was designed using Graphical Network Simulator (GNS3), virtual machines, VMware workstation, firewall, router, and switches in order to examine the attacks on networks in real environment. Attacks were performed on this network with different techniques and target servers and devices were affected by the attacks. At the time of the attack, network traffic between the attacker and the target device was recorded with Wireshark software. Network traffic records and traces were examined and evaluations of attacks were made.

Keywords: Network Attacks, SQL Injection, DDoS, XSS, GNS3, Network Security.

Farklı Türdeki Ağ Ataklarının GNS3 Platformunda Analizi

Öz

Bu çalışmada, bilgisayar korsanlarının siber saldırılarda en fazla kullandığı DDoS, SQL enjeksiyonu ve XSS saldırıları GNS3 emulator platformunda modellenmiş, ağ güvenliği analiz edilmiştir. Ağlara yapılan saldırıları gerçek ortamında inceleyebilmek için Grafiksel Ağ Simülatörü (GNS3), sanal makineler, VMware iş istasyonu, güvenlik duvarı, yönlendirici ve anahtarlar kullanılarak bir ağ senaryosu tasarlanmıştır. Bu ağ üzerinde farklı teknikler ile saldırılar gerçekleştirilmiş, hedef sunucu ve cihazların saldırılardan etkilenmesi sağlanmıştır. Saldırı anında, saldırgan ve hedef cihaz arasındaki ağ trafiği Wireshark yazılımı ile kayıt altına alınmıştır. Ağ trafik kayıtları ve izler incelenerek, saldırılara ait değerlendirmeler yapılmıştır.

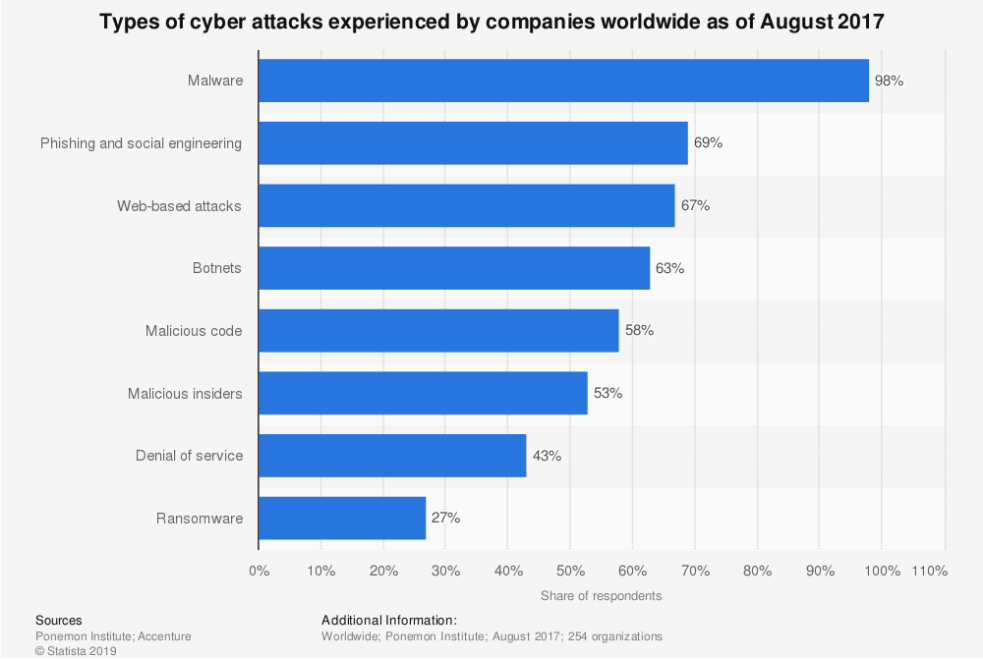
Anahtar Kelimeler: Ağ Saldırıları, SQL Enjeksiyonu, DDoS, XSS, GNS3, Ağ Güvenliği

1. Giriş

Günümüzde İnternet, çalışma ve günlük hayatımızın vazgeçilmez bir parçası haline gelmiştir. İnternet tabanlı sosyal ağlar, IoT(Internet of Things) ve İnternet teknolojilerinde yaşanan hızlı gelişmeler bilgisayar ağlarına yapılan saldırıların artmasına yol açmıştır. Bu nedenle kampüs ağlarının güvenliğini en üst seviyeden kontrol etme zorunluluğunu ortaya çıkartmıştır.

İlk zamanlarda bilgisayar korsanları, kişisel bilgisayar ve ağlara saldırırken duygularını tatmin, idealistlik ve dikkat çekme gibi amaçlar güderken, bu saldırılar günümüzde "Siber Saldırı" veya "Siber Silah" haline gelmiştir.

Bilgisayar korsanları tarafından kullanılan sayısız saldırı türü ve aracı ile bilgisayar ağlarına saldırılar yapılmaktadır. Teknolojinin hızlı gelişmesine paralel olarak yeni saldırı türleri ve yöntemleri ortaya çıkmaktadır. Malware, sosyal mühendislik, casus yazılımlar, şifre kaydediciler(Key Logger), gelişmiş port tarayıcıları, virüsler, yığın e-postalar (Spam), solucanlar, truva atları, arka kapılar (Backdoors), fidye yazılımları (Ransomware), korsan amaçlı kullanılan yazılımlar (Rootkits), zombi makineler, yazılım açıkları ve web uygulamalarındaki kodlama hataları bilgisayar korsanları tarafından kullanılmaktadır. 2017 yılı itibariyle dünya genelinde bildirilen saldırı sayıları Şekil 1'de sunulmuştur.



Şekil 1 2017 yılında gerçekleşen saldırıların dağılım oranları [1]

Kampüs ağlarına ve web uygulamalarına yapılan saldırılar sınıflandırıldığında, Hizmet Aksatma (Denial of Service-DoS), SQL Enjeksiyonu ve XSS (Cross Site Scripting- Çapraz Betik Saldırıları) saldırıları en sık kullanılan saldırı yöntemleri olarak öne çıkmaktadır.

Bilgisayar ağlarına yapılan saldırılar ve yöntemler geliştikçe bu saldırıları engellemeye yönelik yeni yaklaşımlarda ortaya çıkmaktadır. Klasik İmza Tabanlı (Signature-Based Detection) saldırı tespit sistemleri aktif olarak kullanılmakla beraber Anomali Tabanlı Denetim (Anomaly-Based Detection) olarak ifade edilen yeni bir yaklaşım tarzı ortaya çıkmıştır. İmza tabanlı STS'ler daha önceden veri tabanı'na kaydedilmiş bilinen saldırıları tespit etmede yüksek başarı oranına sahipken veri tabanında kayıtlı olmayan veya ilk defa gerçekleşen saldırıları tespit etmekte etkisiz kalmaktadır [2]. Anomali tabanlı STS'leri İmza Tabanlı STS'lerden ayırt eden en önemli özellik ilk defa yapılan veya daha önce kullanılmamış yöntemler ile yapılan saldırıları tespit etmede gösterdikleri yüksek başarı oranıdır. Anomali tabanlı STS'ler normal kullanıcı trafiği ile saldırgan trafiğini ayırt ederek zararlı trafiği engelleyebilme yeteneğine sahiptir.

Bu çalışma ile ağ yöneticilerinin, siber saldırılar karşısında almaları gereken güvenlik önlemleri ve güvenlik politikaları maddeler halinde açıklanmıştır. Ayrıca gerçekleştirilen saldırılar esnasında, ağ trafiğine ait kayıtların nasıl elde edildiği ayrıntılarıyla ifade edilmiştir.

Bu makalenin ikinci bölümü makale kapsamında gerçekleştirilen saldırı uygulama yöntemlerine ait literatür taramasını, üçüncü bölümü kampüs ağlarına gerçekleştirilen güncel saldırı yöntemlerini, dördüncü bölümü ağ senaryoları ve saldırı uygulamalarını, beşinci bölümü çalışmada elde edilen sonuçlara göre saldırılardan korunmak için önerileri, altıncı bölümü sonuçları kapsamaktadır.

2. Literatür Taraması

Bilişim sistemlerinin yaygın ve etkin kullanımı ile ağ güvenlik çözümlerinin önemini her geçen gün arttırmış, bu konusunda da son yıllarda sürekli yeni yaklaşımlar ve çözümler sunulmaktadır. Literatüre ve bilişim firmalarının bu konudaki farklı çözümleri incelendiğinde etkin ve güvenilir yaklaşımlar görülmektedir. Son yıllarda yapılmış çalışmalardan bazıları literatür taraması olarak verilebilir.

[3] nolu çalışmada, yazılım tanımlı ağlarda kantitatif yöntemlerle DoS saldırılarını tespit etmeye çalışmışlardır. DoS saldırılarını incelemek için Mininet platformu kullanılarak, Anomali Tabanlı saldırı tespit ve engelleme stratejisi geliştirilmiştir. Ağ trafiğindeki paket içeriklerinin Entropi ve Jain indekslerini hesaplayarak Jain indeksinin Entropiye göre daha başarılı olduğunu ortaya koymuşlardır.

[4] nolu çalışmada, Yapay Sinir Ağları (YSA) temelli Zeki STS geliştirmeye yönelik çalışmalar yapmışlardır. KDD'99 veri seti kullanılarak 9 temel ve 32 adet türetilmiş olmak üzere toplamda 41 adet özellik haritası çıkartılmıştır. Bu özellikleri 3 temel kategoriye ayırıp, her kategorideki eğitim verisi ile YSA'nı eğitmişlerdir. Eğitim sonucu geliştirilen Zeki STS DoS ve diğer saldırı türlerinden yapılan saldırıları tespit etmede en yüksek %97,92 ve en düşük %81,93 başarı elde etmiştir.

[5] nolu çalışmada ise, ağ iletişim protokollerindeki başlık bilgilerinin değiştirilmesiyle gerçekleştirilen saldırı yöntemleri incelenerek Scapy [6] aracı ile örnek saldırı uygulamaları geliştirmişlerdir.

[7] nolu çalışmada, Ip kamera görüntülerinin iletildiği düşük güvenlikli ağlarda Wireshark yazılımı ile elde edilen kayıtlardan kişisel verilere ve konum bilgilerine kısmi erişim sağlamak üzere örnek çalışma yapmışlardır.

[8] nolu çalışmada, CICIDS2017 veri setine Principal Component Analysis (PCA - Temel Bileşen Analizi) tekniği uygulanarak veri boyutunu azaltıp, sınıflandırıcı algoritmalar ile sınıflandırmaya uygun hale getirmişlerdir. Elde edilen yeni veri seti ile sınıflandırıcılar kullanılarak, STS geliştirmişlerdir [8].

[9] nolu çalışmada, gerçek zamanda çalışan FPGA (Field Programmable Gate Array - Alan Programlanabilir Kapı Dizileri) tabanlı programlanabilir gömülü bir STS'nin tasarımı için 4 adımdan oluşan bir mimari geliştirilmişlerdir. Ağdan yakalanan paketler normalize işlemine tabi tutularak YSA'da girdi veri seti olarak kullanılmıştır. YSA giriş ve ara katmanda Hiperbolik Tanjant Sigmoid, çıktı katmanında Lineer Transfer fonksiyonları kullanılarak çıktı katmanında paketin saldırımı yoksa normal ağ trafiği olduğuna karar vermişlerdir. Gerçek zamanda yapılan testlerde 2000 paketin 392'si Saldırı1, 297'si Saldırı2 ve 1311'i Normal paket olarak tespit etmişlerdir.

[10] nolu çalışmada, OSI modelinin farklı katmanlarına değişik tipte yapılan DDoS saldırılarının tespiti, önlenmesi ve DDoS saldırılarının bulut bilişime olan etkileri üzerine çalışmalar yapmışlardır. DDoS'un bulut ağı uygulama ve ağ katmanı ile OSI katmanları üzerindeki etkisini, araştırmacıların kullandığı olası çözümleri araştırmışlardır. Her bir yaklaşımın avantajları, dezavantajları ve DDoS'un bulut ağında ortaya çıkarttığı sorunları tanımlamışlardır.

[11] nolu çalışmada, SQL Enjeksiyon saldırıları 4 ana kategoride 22 farklı teknik ile incelenerek SQL sorgularının, SQL enjeksiyon saldırılarında nasıl uygulandığını detaylı şekilde açıklamışlardır.

[12] nolu çalışmada, ASP.NET-MS SQL tabanlı web uygulaması üzerinde, SQL enjeksiyon saldırı analizi yapılarak güvenlik zafiyetleri ortaya koyulmuş ve SQL enjeksiyon saldırılarından korunmak için öneriler sunmuşlardır.

[13] nolu çalışmada, Grafiksel Ağ Simülatör Yazılımı (GNS3), Oracle Virtual Machine(Sanal Makine), VMware iş istasyonu ve Wireshark gibi birçok açık kaynak kodlu yazılım kullanarak silahsızlaştırılmış bölge (DMZ – Demilitarized Zone) ağ ortamı tasarlamışlardır. Tasarlanan ağ'da SQL enjeksiyon saldırısı gerçekleştirerek, saldırı anındaki ağ paketleri kayıt altına alınmıştır. Uygulama sonucu elde edilen ağ kayıtları kullanılarak SQL enjeksiyon saldırısı tespit metodolojisi tanımlamışlardır.

[14] nolu çalışmada, Web uygulamalarındaki XSS açıkları Asp.NET, PHP, PHP ve Ruby programlama dilleri ile farklı platformlarda uygulamalı olarak analiz edilmiş ve çözüm önerilerini sunmuşlardır.

[15] nolu çalışmada, XSS ve SQL enjeksiyon saldırılarının zararlı etkilerinden korunmak ve saldırgan kimliği hakkında bilgiler toplayabilmek için düşük etkileşimli bal küpü modeli üzerinde çalışma yapmışlardır. 2 aylık test sürecinden sonra bal küpü modeli ile sadece saldırı tespiti değil aynı zamanda saldırganın kimliği hakkında da bilgi toplamayı başarmışlardır. Ayrıca saldırgan, saldırı anında kimliğini gizlemek için proxy veya TOR kullanmasına rağmen, LikeJacking tekniğini ile yakalanan saldırganın sosyal medya hesapları hakkında bilgi tespit edebilmişlerdir.

[16] nolu çalışmada, SQL Enjeksiyonu, XSS saldırıları, Wordpress kullanıcı adı çalma ve kablosuz erişim şifrelerinin ele geçirilmesi senaryolarını Kali Linux İşletim sistemini kullanarak simüle etmişlerdir. SQL enjeksiyonu saldırısı için sqlmap aracından yararlanılmıştır. XSS saldırısında, yalnızca istismar edilen web sunucusundan yararlanmayı değil, aynı zamanda web sunucusuna uzaktan erişim sağlayan kurban PC'ye uzaktan erişim sağlanmayı başarmışlardır.

Tablo 1 DDoS, SQL enjeksiyonu, XSS saldırısı inceleme çalışmaları

Ref.	Çalışmanın Amacı	Saldırı Tipi	Kullanılan Metot	Platform	Sonuç
[3]	DoS Saldırılarının Tespiti	DoS / DDoS	Entropi -Jain indeksi	Mininet	Jain İndeksi Entropiye Göre Daha Yüksek Başarım Oranı
[4]	YSA Temelli Zeki STS Tasarımı	DoS / DDoS	1 Giriş, 2 Ara Katman ve Çıkış Katmanlı YSA	-	En Yüksek %97,92 En Düşük %81.93
[6]	Protokol Bazlı Saldırı Türlerinin Analizi	DoS / DDoS	Flooding	Scapy	Flood Saldırıları Gerçekleştirmiştir
[7]	Wireshark ile Paket Analizi	Sniffing	UDP	Wireshark	Wireshark ile Ağ Trafiği ve Konum Tespiti
[8]	PCA Tekniği İle STS Tasarımı	DDoS, Brute Force, XSS, SQL Enjeksiyonu, Botnet	CICIDS2017 Veri Seti	IDS	PCA Tabanlı STS Geliştirilmiştir.
[9]	FPGA tabanlı STS Tasarımı	-	YSA Temelli Saldırı Tespit Sistemi	IDS	Normal Ağ Trafiği ile Saldırı Trafiği Tespiti
[10]	DDoS Saldırılarının Bulut Bilişime Etkileri	DDoS	Saldırıların Bulut Teknolojisine Etkileri ve Çözüm Önerilerinin Karşılaştırılması	IDS	DDoS'un OSI Katmanlarına Etkileri
[11]	SQL Enjeksiyon Saldırılarının Önlemesi	SQL Manipülasyonu, Kod Enjeksiyonu, Fonksiyon Çağrı Enjeksiyonu, Tampon Taşması	22 Farklı Teknik İle Saldırı Tespiti		SQL Enjeksiyon Saldırılarının Kategorizasyonu
[12]	SQL Enjeksiyon Açıklarının a Karşı	SQL Manipülasyonu	Web Uygulamasına SQL Enjeksiyon Saldırısı	ASP.NET, MS SQL	SQL Saldırılarından Korunma Yöntemlerinin Sınıflandırılması
[13]	SQL Enjeksiyon Saldırılarını GNS3 Kullanarak Simüle Etme	SQL Enjeksiyonu	GNS3 İle DMZ Ağ'a SQL Enjeksiyon Saldırısı Simülasyonu	GNS3	SQL Enjeksiyon Saldırısı Tespit Metodolojisi Önerilmiştir
[14]	XSS Ataklarının Tespiti	XSS Saldırısı	Asp.NET, PHP, PHP ve Ruby İle XSS Analizi	-	XSS Saldırılarının Kategorizasyonu ve Saldırıları Tespit Ederek Başarı Oranları Karşılaştırılmıştır
[15]	Bal Küpü Tekniği İle Saldırı Tespiti	XSS ve SQL Enjeksiyon Saldırısı	Düşük Etkileşimli Bal Küpü Modeli	SQLMap, Likejacking	Saldırı Tespiti ve Saldırganın Sosyal Medya Hesapları Tespit Edilmiştir
[16]	Penetrasyon Testi	XSS, SQL Enjeksionu, Wordpress ve WPA2 Saldırısı	Kali Linux İle SQL Enjeksiyonu, XSS, Wordpress ve Kablosuz Erişim Şifrelerinin Ele Geçirilmesi Saldırıları Simüle Edilmiştir	Kali Linux	Güvenlik Açıkları Tespit Edilerek WPA2 Protokolü Kullanan Kablosuz Erişim Şifresi Ele Geçirilmiştir

3. Ağ Saldırlarının İncelenmesi

Bu bölümde ağlara yapılan saldırılar incelenerek saldırılar kendi içinde saldırı türlerine göre gruplara ayrılmıştır. Gruplara ayrılan saldırı türleri hakkında genel hatlarıyla bilgi verilmiştir.

3.1. DoS/DDoS Saldırısı

DoS, tek makine ile bir web hizmet servisini başka bir faaliyetle meşgul ederek servisin hizmet vermesini engellemeye yönelik saldırı olarak tanımlanmaktadır. Web hizmeti, saldırı sonucu kesintiye uğradığında isteklere yanıt veremez duruma gelmektedir. İnternet'ten çevrimiçi alınan sağlık hizmetleri, kurumsal hizmetler, sosyal ağ, eğitim, finansal ve bankacılık işlemleri dikkate alındığda web hizmetlerinin aksamadan yerine getirilmesi günümüzde hayati önem arz etmektedir.

Birden fazla makine ile gerçekleştirilen DoS saldırısına DDoS saldırısı denilmektedir. DDoS saldırı ile hedeflenen makineye veya sistemin kaynakları aşırı tüketilerek saldırının yıkıcı gücü artmaktadır. DoS veya DDoS saldırının nihai hedefi, ağ trafiğini aşırı yükselterek sistemin çok miktarda kaynak kullanmasını sağlamak ve hizmetin aksamasını sağlamaktır [17].

3.2. Enjeksiyon Saldırıları

Web uygulamalarına veri girişi yapılan metin kutuları veya uygulama parametrelerine bilgisayar korsanları tarafından yerleştirilen komut yada sorgu parçasının yorumlayıcıda çalışmasını sağlayarak gerçekleştirdikleri saldırılara enjeksiyon saldırı denilmektedir [18].

Saldırgan yorumlayıcıda çalışacak hale getirdiği kod parçalarını veri girişi yapılan alanlardan göndererek okuma, yazma veya silme gibi eylemleri izinsiz olarak gerçekleştirebilmektedir. Ayrıca işletim sisteminde çalışan kodlar göndererek sunucu veya silahsızlandırılmış DMZ alanlarına erişim sağlayabilmektedir.

3.3. SQL Enjeksiyon Saldırısı

E. F. Codd'un Haziran 1970 yılında Association of Computer Machinery (ACM) dergisinde yayınlanan "Büyük Paylaşımlı Veri Bankaları için İlişkisel Veri Modeli" makalesi ilişkisel veri tabanı yönetim sistemlerinin (RDBMS) temeli kabul edilmektedir [19]. SQL (Structured Query Language), 1975 yılında IBM firması tarafından ANSI (American National Standards Institute) standartlarına uygun olarak yapısal sorgulama dilidir. SQL cümleleri ile veri tabanında veri ekleme, silme, güncelleme ve arama işlevleri yerine getirilmektedir.

SQL enjeksiyon saldırısı, kullanıcının web uygulamasına veri girişi yaptığı zaman arka planda oluşturulan SQL cümlelerini manipüle etmesiyle gerçekleştirilir. Başarılı bir SQL enjeksiyon saldırısı, veri tabanındaki kritik verileri okuyabilir, değiştirebilir veya silebilir [12].

3.4. XSS Saldırısı

Siteler Arası Çapraz Betik Saldırıları, kullanıcılar tarafından güvenilir olarak düşünülen web sitelerine zararlı kodlar eklenerek gerçekleştirilen saldırı yöntemidir [14]. Bilgisayar korsanı veya saldırgan tarafından web uygulamalarına yerleştirilen zararlı kodların, normal kullanıcı(kurban) tarayıcısında izinsiz çalıştırılması sonucu istemci çerezleri veya kullanıcının site erişim bilgileri ele geçirilerek normal kullanıcıyı taklit etmesini sağlar. Oturum Çalma, Yanlış Bilgilendirme, Web Sitesine Ekleme, Açılır Pencere ve Web Sitesine Zararlı Kod Gömme olmak üzere farklı saldırı yöntemleri mevcuttur.

3.5. Kod Enjeksiyon Saldırısı

HTML5 programlama dili ile geliştirilen web ve mobil uygulamaların veri giriş alanlarına yerleştirilen kod'lar aracılığıyla gerçekleştirilen saldırı yöntemidir [20],[21]. Mobil uygulamalarda çok fazla veri giriş alanı (wi-fi, kısa mesaj, kişi rehberi vb.) bulunması nedeniyle kod enjeksiyon saldırıları için uygun zemin oluşmakta ve saldırılar ile sistemler istismar edilmektedir.

3.6. XPath Enjeksiyon Saldırısı

XML Path Language (XPATH) XML dokümanları içinde sorgu yapmak için kullanılan yorumlayıcı sorgulama dilidir. Web uygulamaları genellikle veri, konfigürasyon veya parametre verilerini saklamak

için XML dosyalarını kullanır. XML dosyaları üzerinde işlem yapılırken XPATH enjeksiyon saldırıları için önlem alınmamışsa; Düğümlere erişmek için kullanılan sorgu komutları ile XML veritabanındaki tüm verilere ulaşmak mümkün olacaktır. XML verilerine ulaşıldıktan sonra hak yükseltme ve diğer veritabanlarına erişim gibi daha yıkıcı saldırılar ile karşı karşıya kalınmaktadır [22].

3.7. Sosyal Mühendislik Saldırıları

En temel saldırı yöntemlerinden biri olan Sosyal Mühendislik Saldırısı, insani zaaflardan veya dikkatsizliklerden faydalanarak, kurumsal ağ ve kurum personeli hakkında çeşitli bilgiler elde etmek, şifreleri ele geçirmek veya saldırılara ön hazırlık yapmak amacıyla her türlü verinin elde edilmesi sürecini ifade etmektedir.

Telefon aracılığıyla aldatma, çöpleri karıştırma, güvenilir kaynaktan gönderildiği hissi oluşturan mesajlar ile ikna etme(oltalama), truva atları (trojan), tersine mühendislik, eski cihazlar üzerindeki depolama birimlerinde kalan verilerin ele geçirilmesi, ödül avcılığı, oltalama, omuz sörfü, tanınmış kişiler adına açılan sahte sosyal medya hesapları ile aldatma yöntemleri sosyal mühendislik saldırılarında en sık başvurulan saldırı yöntemleridir [23].

3.8. Honeypot(Bal Küpü) Temelli Saldırılar

Bilgisayar korsanları veya yetkisiz erişim sağlamaya çalışan saldırganlar hakkında bilgi toplamak amacıyla kurulan özel tuzak sunuculara honeypot(bal küpü) denir [24],[25]. Bal küpleri ağın bir parçası olarak faaliyet gösteren sunucu veya ağ cihazı olabilir. Bal küpü sahte veriler, dokümanlar, hayali kimlik bilgileri, şifre veya kredi kartı bilgileri gibi saldırganların dikkatini çekecek veriler barındırır. Üzerinde farklı seviyelerde güvenlik açıkları bırakılan bal küpleri saldırganların öncelikli hedefi haline gelmesi sağlanır.

Hedef bal küpüne yapılan saldırılar incelenerek saldırganın kimliği, saldırının kaynağı, yeni saldırı türleri veya yöntemleri tespit edilerek güvenlik cihazlarına alarm üretmesi sağlanır. Ağda yerleştirildikleri konuma göre Üretim bal küpleri (production honeypots) ve Araştırma bal küpleri (research honeypots) olmak üzere iki gruba ayrılır [25].

Araştırma balküpleri saldırganlar tarafından kullanılan yeni saldırı tekniklerini araştırmak ve tespit etmek amacıyla akademik, kurumsal veya amatör amaçlarla kullanılan basit sistemlerdir. Oltalama şeklinde saldırganları çeken sistemler de denilebilir.

Üretim balküpleri ise üzerinde çalıştıkları sistemin kopyasını alarak FTP, HTTP, SMTP gibi servislerde bırakılan güvenlik açıkları ile gerçek sistemlere yönelmesi muhtemel tehditleri kendi üzerlerine çekerek gerçek sistemlerin zarar görmesini engellerler [26].

4. Ağ Senaryoları ve Saldırı Uygulamaları

Ağ simülasyon ve emülasyon araçları, son kullanıcıların ve ağ yöneticilerinin karmaşık ağları kısa sürede daha düşük maliyetlerle taklit etmelerini sağlar. GNS3; Linux, Windows ve MAC işletim sistemlerinde çalışabilen açık kaynak kodlu Grafiksel Ağ Simülatör yazılımıdır. GNS3 farklı işletim sistemleri ve Cisco IOS'ların emülasyonunu taklit edebilmektedir [27]. Bu kapsamında Şekil 2'de sunulan sanal test ortamı tasarlanarak 3 farklı saldırı senaryosu gerçekleştirilmiştir. OSI katmanlarına göre farklı saldırı teknikleri kullanılmış ve her saldırı anında oluşan ağ trafiği wireshark yazılımı ile kayıt altına alınmıştır. Kampüs ağının tasarımında aşağıdaki yazılım ve donanım kullanılmış, router, switch, firewall ve sanal pc konfigürasyonları tamamlanarak sanal ağ hazır hale getirilmiştir.

- GNS3 2.2.2 Yazılımı
- VMware Workstation 12 Pro
- GNS3 2.2.2 Virtual Server Yazılımı
- PfSense 2.4.4 Open Source Firewall

- Wireshark 3.0.6
- Kali Linux İşletim Sistemi
- Linux Mint İşletim Sistemi
- Windows 7 İşletim Sistemi
- GNS3 Virtual PC
- Cisco 3725 Router
- Cisco 3640 Router + EtherSwitch

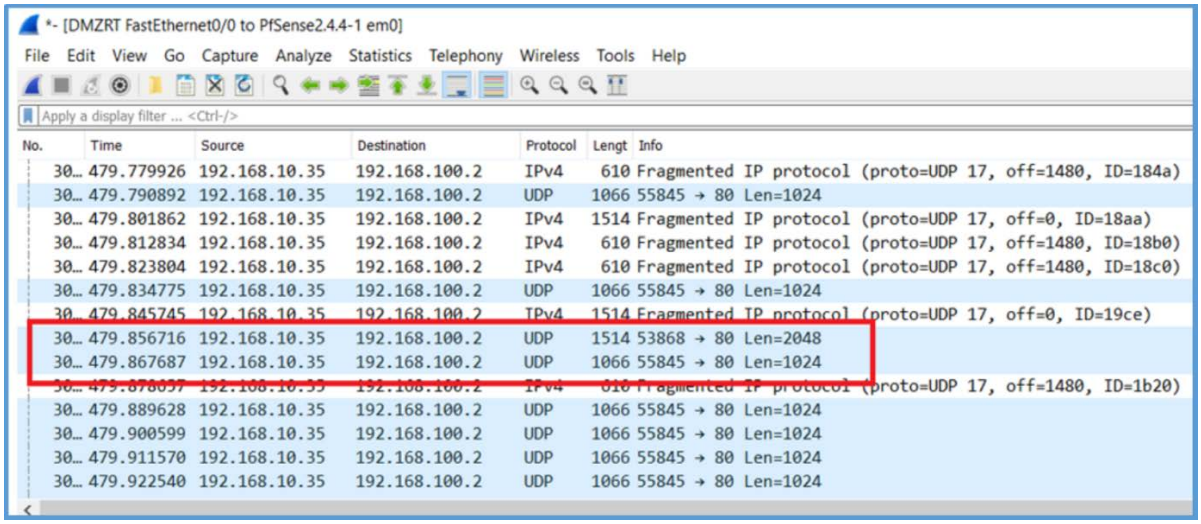
Makale kapsamında, farklı saldırı teknikleri incelenerek saldırılar hakkında genel bilgiler verilmiştir. Ayrıca bilgisayar korsanlarının ağ sistemlerine saldırılarda en sık kullandığı DDoS, SQL enjeksiyonu ve XSS saldırıları GNS3 platformunda modellenerek, saldırılar uygulamalı olarak gerçekleştirilmiştir. Saldırıların ağ'da bıraktığı hasarların sonuçları tespit edilerek saldırılardan korunmak için öneriler sunulmuştur. Tasarlanan ağ, gerçekleştirilen saldırılar ve diğer tüm uygulamalar için kullanılan sisteme ait teknik özellikler Tablo 2'de sunulmuştur.

Tablo 2 Çalışmaların gerçekleştirildiği sisteme ait teknik özellikler

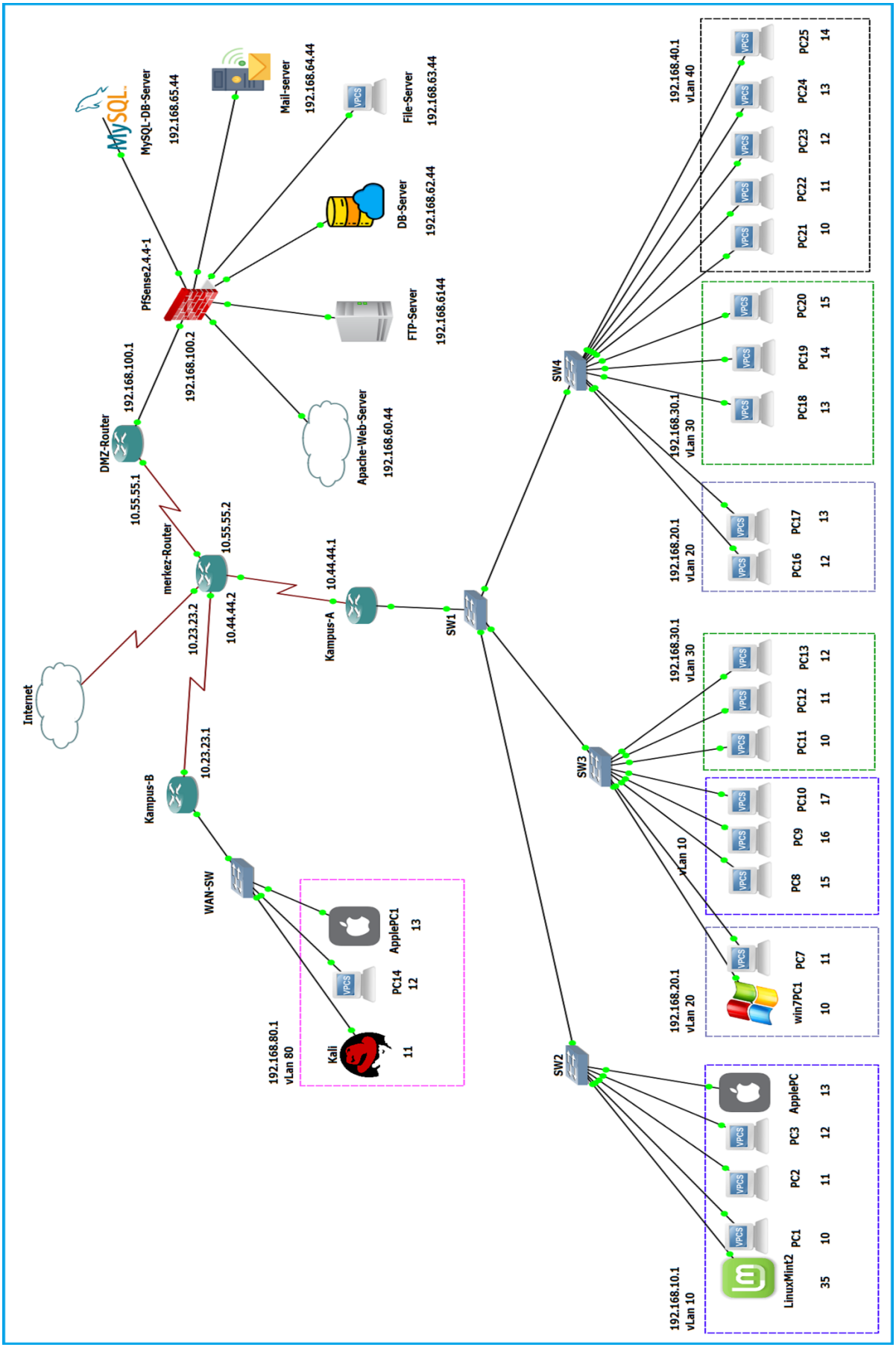
Yazılım / Donanım Adı	Özelliği
İşlemci	Intel Core i7-6700HQ CPU
RAM	16 GB PC4-19200 DDR RAM (2 * 8 GB)
Ekran Kartı	4 GB NVIDIA GeForce GTX 960M
Harddisk	128 GB Toshiba SSD 1 TB Toshiba 5400 Rpm SATA Disk
Ethernet Kartı	Realtek RTL8168/8111 PCI-E Gigabit Ethernet NIC Atheros/Qualcomm AR9462 Wireless Network Adapter
İşletim Sistemi	Windows 10 Home Single Language

4.1. DDoS Saldırı Uygulaması

İlk uygulama**,** kampüs-A ağındaki 192.168.10.35 ip adresine sahip Linux Mint PC'den DMZ alanına hizmet veren 192.168.100.2 ip adresli güvenlik duvarına 2048 ve 1024 byte'lık iki farklı DDoS saldırısı gerçekleştirilmiştir. Her iki saldırı için Perl dilinde hazırlanmış UDP protokolünü kullanan saldırı script'leri kullanılmıştır. Gerçekleştirilen saldırılara ait ağ trafiği Şekil 3'de sunulmuştur.

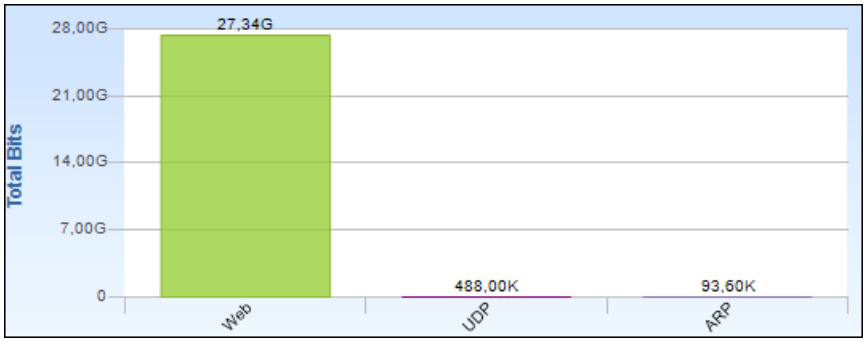


Şekil 3 Güvenlik duvarına yapılan saldırı trafiği



Şekil 2 Saldırı senaryolarının gerçekleştirildiği ağ yapısı

İkinci uygulama; DMZ alanındaki 192.168.60.44 ip adresli apache-web-server'dan 192.168.62.44 ip adresli db-server'a 1024 ve 2048 byte'lık 2 farklı DDoS saldırı olarak gerçekleştirilmiştir. Kayıt altına alınan ağ trafiği Steel Center Packet Analyzer 10.9.3 yazılımı ile analiz edilerek saldırının boyutu Şekil 4'de gösterildiği gibi 27 GB olarak tespit edilmiştir. Saldırı sonucu db-server'a ait normal ağ trafiği tamamen ARP yayınına dönüşerek, HTTP Portu üzerinden iletişim kesilmiştir.



Şekil 4 DDoS saldırı trafik miktarı

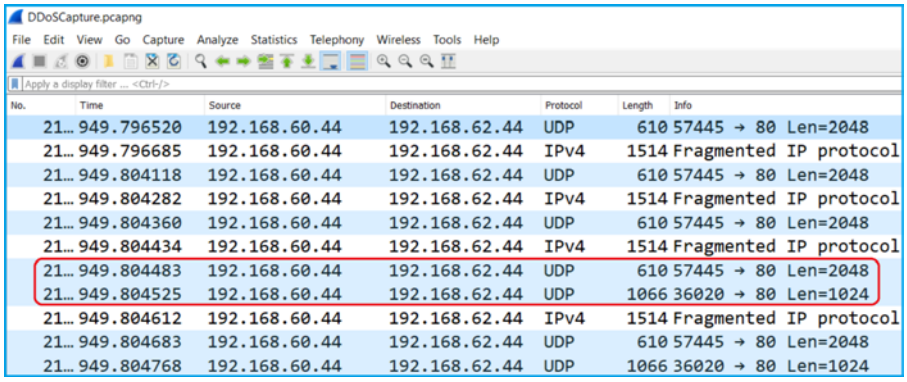
İlk DDoS saldırı uygulaması sırasında PfSense güvenlik duvarı, kendisine yapılan saldırıları algılayıp Şekil 5'te belirtilen kural tablosuna engelleyici kuralları ekleyerek saldırılarının güvenlik duvarının arkasına geçmesine izin vermemiştir.

Last 50 Firewall Log Entries. (Maximum 50)

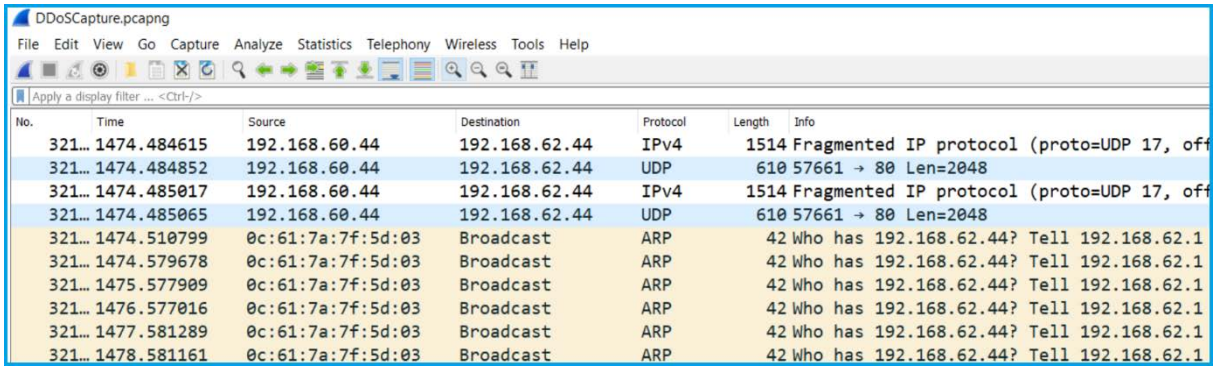
Action	Time	Interface	Rule	Source	Destination	Protocol
✖	Dec 22 16:59:30	WAN	Default deny rule IPv4 (1000000103)	192.168.10.35:40379	192.168.100.2:80	UDP
✖	Dec 22 16:59:30	WAN	Default deny rule IPv4 (1000000103)	192.168.10.35:40379	192.168.100.2:80	UDP
✖	Dec 22 16:59:30	WAN	Default deny rule IPv4 (1000000103)	192.168.10.35:40379	192.168.100.2:80	UDP
✖	Dec 22 16:59:30	WAN	Default deny rule IPv4 (1000000103)	192.168.10.35:40379	192.168.100.2:80	UDP
✖	Dec 22 16:59:31	WAN	Default deny rule IPv4 (1000000103)	192.168.10.35:40379	192.168.100.2:80	UDP
✖	Dec 22 16:59:31	WAN	Default deny rule IPv4 (1000000103)	192.168.10.35:40379	192.168.100.2:80	UDP
✖	Dec 22 16:59:31	WAN	Default deny rule IPv4 (1000000103)	192.168.10.35:40379	192.168.100.2:80	UDP

Şekil 5 Güvenlik duvarı kural tablosu

İkinci DDoS saldırı uygulamasında; saldırı esnasında ağ trafiği Şekil 6'da belirtildiği gibi wireshark yazılımı ile kayıt altına alınarak incelendiğinde, saldırıların hangi protokolle gerçekleştirildiği, saldırıların kapasitesi, süresi, boyutu, saldırının kaynağı ve hedefi açıkça tespit edilmiştir. Saldırı sonunda db server'e ait ağ iletişimi Şekil 7'de belirtildiği üzere ARP yayınına dönerek HTTP iletişimi kesilmiş ve Şekil 8'de sunulduğu gibi tüm veri trafiğinin sonlanmasına neden olup db server'in hizmet aksatması sağlanmıştır.

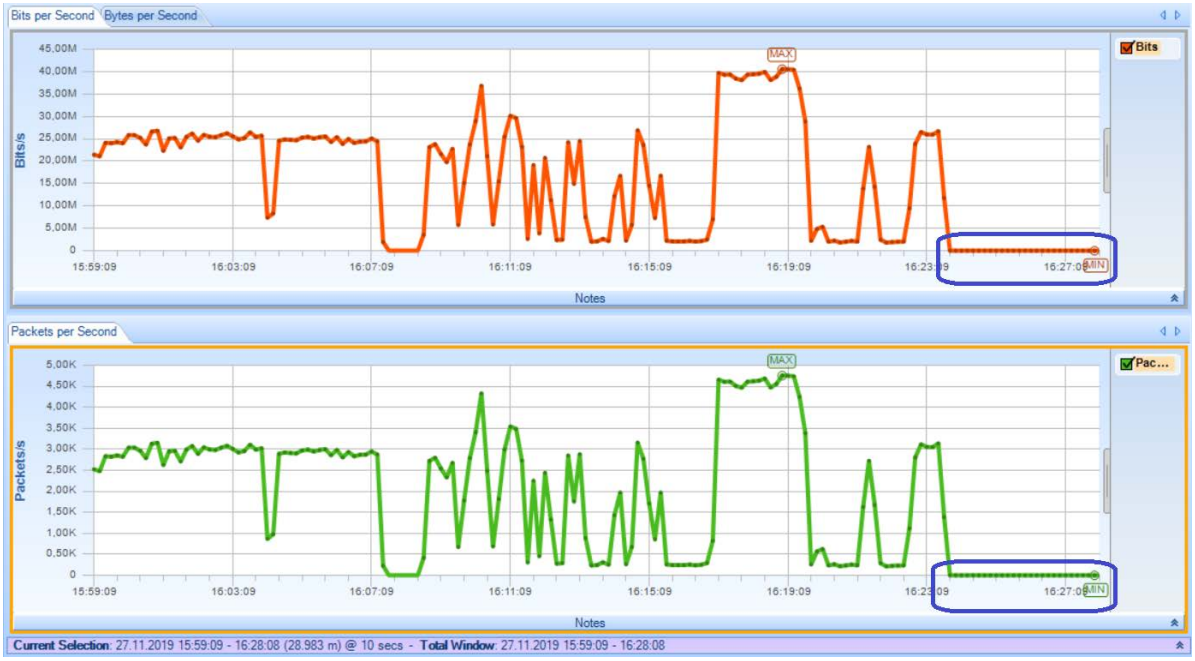


Şekil 6 Db server'e yapılan saldırı trafiği



Şekil 7 Saldırılar sonucu db-server ağ trafiği

Gerçekleştirilen iki farklı DDoS saldırısı ile hedef sistemin 80 nolu portuna 1.187.425 adet 2048 byte ve 439.167 adet 1024 byte olmak üzere toplam 2.68 GB'lık UDP paketi gönderilerek sunucunun devre dışı kalması sağlanmıştır.



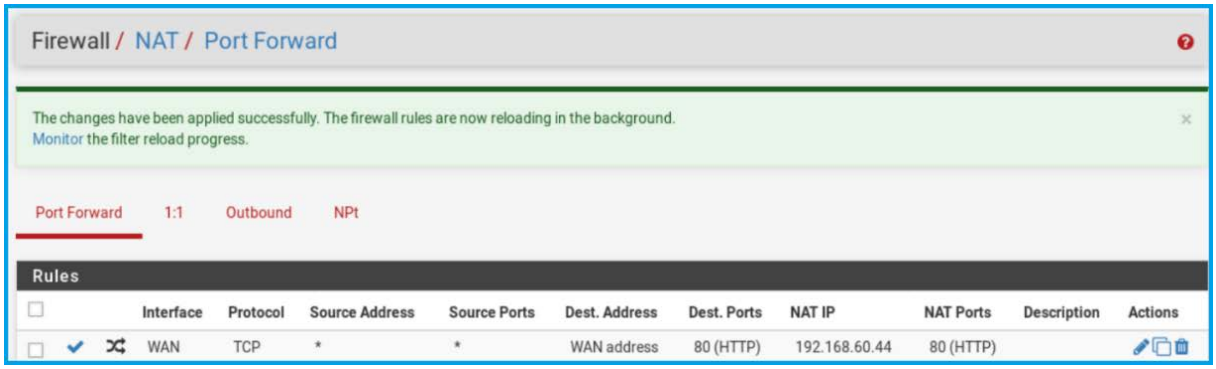
Şekil 8 Saldırı anında ağ trafiğinin sonlandığına ait bit ve packet grafiği

4.2. SQL Enjeksiyon Saldırı Uygulaması

Damn Vulnerable Web Application (DVWA), içeriğinde farklı güvenlik seviyeleri olan, MySQL veri tabanı ve PHP dili kullanılarak yazılmış web uygulamasıdır. DVWA uygulaması SQL Enjeksiyon ve XSS saldırıları gerçekleştirilebilecek açıkları barındırmaktadır. Bu açıklıklar web uygulamalarını güvence altına alma süreçlerini daha iyi anlayabilme, yönetebilme ve sınıf içi bir ortamda web uygulama güvenliğini öğretme/öğrenme konusunda yardımcı olmakla beraber web güvenliği test araçlarının yasal ortamda test edilmelerine imkan sunmaktadır[28]. Bu nedenle SQL Enjeksiyon saldırıları için DVWA web uygulaması kullanılmıştır.

DMZ alanında apache-web-server'inde yayın yapan DVWA web sitesine; 192.168.10.35 ip adresli adresinde Linux Mint PC'den SQL injection saldırısı yapılarak veri tabanında kayıtlı verilere erişilmeye çalışmıştır. DVWA web uygulaması, DMZ alanında yayın yaptığı için güvenlik duvarı arkasından dış kullanıcıların apache-web-server'e erişebilmesi güvenlik duvarına ait wan ara yüzü 80 numaralı portuna gelen isteklerin apache-web-server'e NAT (Network Address Translation) yapılarak yönlendirilmesi

gerekmektedir. Güvenlik duvarına NAT kaydı eklenip ağ kullanıcılarının web uygulamasına erişmesi sağlanmıştır, Şekil 9'da güvenlik duvarına eklenen NAT kaydı görülmektedir.



Şekil 9 Güvenlik duvarı NAT kaydı

Web uygulamasına erişim sağlandıktan sonra adım adım SQL Enjeksiyon saldırısı yapılarak veri tabanında kayıtlı verilere ulaşılmıştır.

Adım-1: SQL enjeksiyon açığı olup olmadığını tespit etmek için Şekil 10'da belirtilen User Id alanına tek tırnak (') karakteri girilerek sayfanın SQL injection açığı kontrol edilmiş ve Şekil 11'de belirtildiği gibi hata mesajı alınarak SQL enjeksiyon açığı tespit edilmiştir.

Şekil 10 SQL enjeksiyon açığı kontrolü

Şekil 11 Sorgu sonucu ekrana gelen hata mesajı

Adım-2: SQL enjeksiyon açığı tespit edildikten sonra, sırasıyla Kod 1'de sunulan SQL komutları User ID alanından uygulamaya gönderilerek veri tabanı ve tablolar hakkında çeşitli bilgiler elde edilmiştir.

Kod 1 SQL enjeksiyon kodları

```
44' or '1' = '1' # //SQL sorgusunun çalıştığı tablodaki kayıtları aldık
44' or '1' = '1' ORDER BY 1 # // SQL sorgusundaki alanlardan 1. alana göre kayıtları sıralı getirir
44' or '1' = '1' ORDER BY 2 # // SQL sorgusundaki alanlardan 2. alana göre kayıtları sıralı getirir
44' or '1' = '1' ORDER BY 3 # // Unknow column '3' in 'order clause' hatası alındı, geri planda çalışan SQL sorgusunda 2 alan select edilmiş demektir!
```

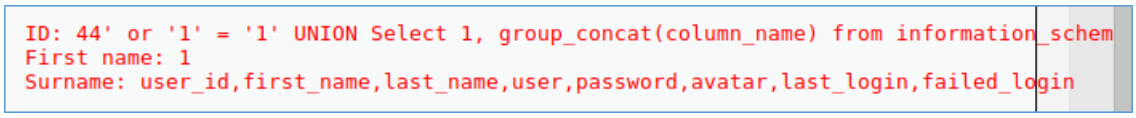
Kod 1 SQL enjeksiyon kodları (*devamı*)

44' or '1' = '1' UNION Select 1,version() # // *Listelenen kayıtların son satırında çalışan DB versiyonunu aldık :* **10.3.15-MariaDB-1**

44' or '1' = '1' "UNION Select 1,group_concat("schema_name") from "information_schema.schemata" # *//web uygulamasında çalışan veri tabanı isimlerini listeledik* **"informaion_schema", "dvwa"**

44' or '1' = '1' UNION Select 1,group_concat(table_name) from information_schema.tables Where table_schema='dvwa' # *// tespit ettiğimiz veri tabanındaki tabloların isimlerini listeledik* **"users", "uestbook"**

44' or '1' = '1' UNION Select 1,group_concat(column_name) from information_schema.columns Where table_name='users#' *//users tablosundaki alan adları listesi* Şekil 12'de *sunulmuştur.*

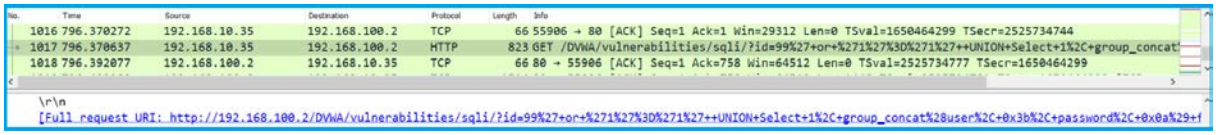


Şekil 12 User tablosu alan adları

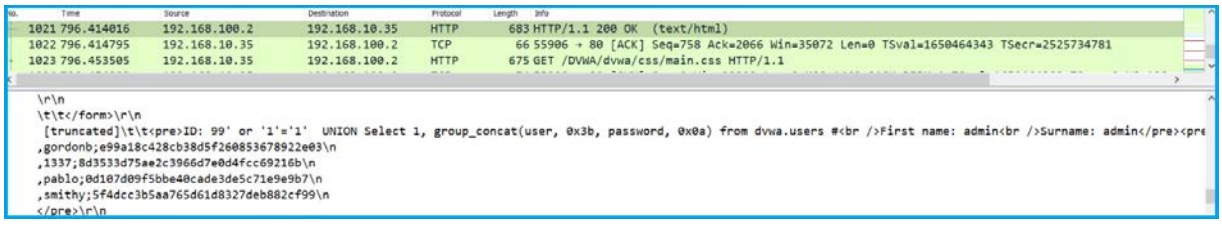
Adım-3: Bilgi toplama adımlarının sonunda "44' or '1' = '1' UNION Select 1, "group._concat"(user,0x3b,password,0x0a) from dvwa.users #" SQL kodu gönderilerek "users" tablosunda kayıtlı kullanıcı adı ve şifre özetleri Şekil 13'de belirtildiği şekilde ele geçirilmiştir.

Şekil 13 User tablosu şifre özetleri

SQL enjeksiyon saldırısı boyunca ağ trafiği wireshark yazılımı ile kayıt altına alınarak incelendiğinde, SQL enjeksiyon saldırı istek kodları Şekil 14'te ve web sunucusunun verdiği yanıtlar Şekil 15'te sunulmuştur.



Şekil 14 SQL enjeksiyon istek kod trafiği



Şekil 15 Web server talep edilen sql isteğine verilen cevap kod trafiği

SQL enjeksiyon saldırısına uğrayan veritabanında kayıtlı kullanıcı adı ve şifre özetleri hash kod çözücü uygulamalar ile işleme alındıktan sonra elde edilen şifrelere ait bilgiler Tablo 3'de sunulmuştur.

Tablo 3 Veritabanında kayıtlı hash kod özetleri ve şifre tablosu

Kullanıcı Adı	Hash Kodu	Şifre
admin	5f4dcc3b5aa765d61d8327deb882cf99	password
gordonb	e99a18c428cb38d5f260853678922e03	abc123
1337	8d3533d75ae2c3966d7e0d4fcc69216b	charley
pablo	0d107d09f5bbe40cade3de5c71e9e9b7	letmein
smithy	5f4dcc3b5aa765d61d8327deb882cf99	password

SQL enjeksiyon saldırısının amacına ulaşması için uygulamaya 15 defa enjeksiyon kodlarını içeren istekler gönderilmiş ve uygulamadan gelen cevaplar doğrultusunda Tablo 3'de belirtilen bilgilerin elde edilmesi sağlanmıştır.

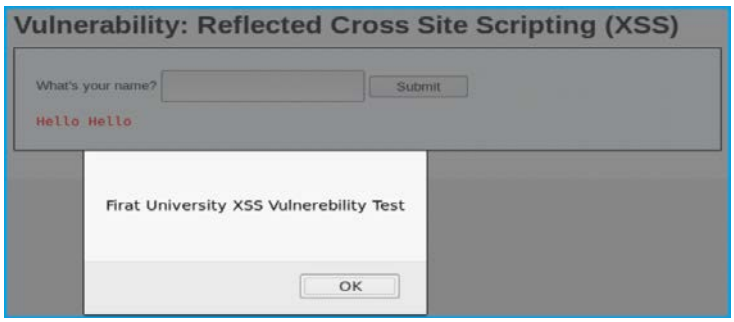
4.3. XSS Saldırı Uygulaması

Makale kapsamında XSS saldırı yöntemleri arasından "Web Sitesine Zararlı Kod Gömme" yöntemi kullanılarak uygulama gerçekleştirilmiştir. Bu yöntem ile bilgisayar korsanı XSS açığı bulunan web sitesine; Kullanıcılara veya web uygulamasına zarar verecek kodları önceden yerleştirmektedir. Bilgisayar korsanı tarafından önceden yerleştirilen zararlı kodlar, normal kullanıcı ziyareti sırasında arka planda çalıştırılarak kullanıcıların oturum bilgileri ele geçirilmekte, verileri çalınmakta veya saldırıya maruz kalan web sitesi çalışmaz hale getirilmektedir.

XSS saldırılarını gerçekleştirebilmek için üzerinde farklı XSS açıkları barındıran DVWA Web Uygulaması kullanılmıştır. Kurbanın XSS saldırısına maruz kalması için saldırgan PC'de(vLan80 ağındaki 192.168.80.11 ip adresli Kali PC) XSS açığı bulunan DVWA web uygulaması aktif hale getirilmiştir.

Adım-1: DVWA uygulaması üzerinden XSS açığını test etmek için XSS Reflected modülünde **What's your name?** metin kutusuna **"Hello"** yazılarak submit edilmiştir. Submit işlemi sonunda metin kutusunun altına "Hello Hello" yazdığı görülmüştür. Web uygulmasının kullanıcıdan aldığı bilgiyi paratmetre olarak kabul ettiği ve yorumlayarak ekrana yazdığı görülmüştür.

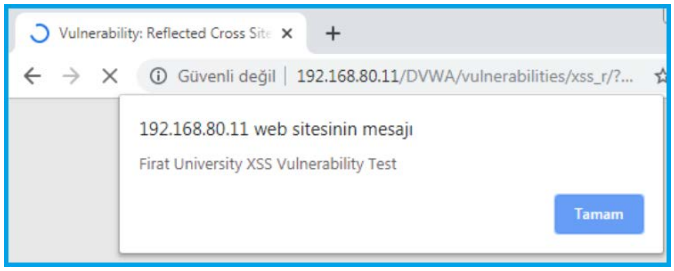
Adım-2: Metin kutusuna **<script>alert("Firat University XSS Vulnerability Test")</script>** JS kod parçası enjekte edilerek kodun tarayıcıda çalışması sağlanmıştır. Zararlı kodu çalıştığı uygulamaya ait ekran görüntüsü Şekil 16'da sunulmuştur.



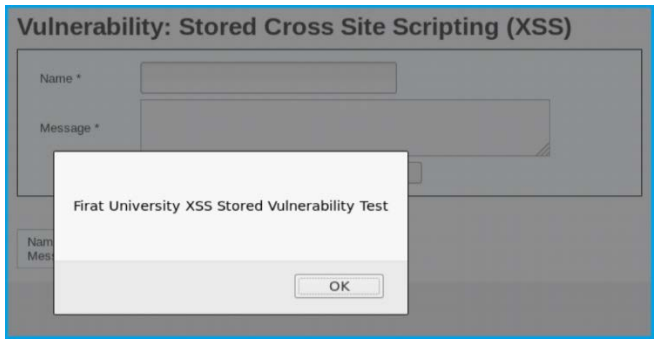
Şekil 16 JS kodu enjekte edilmiş web uygulaması

Adım-3: Zararlı kodların enjekte edildiği web uygulaması vLan20 ağındaki 192.168.20.10 ip adresli Windows 7 sanal PC'den açılarak Şekil 17'de sunulduğu gibi tarayıcıdan uyarı mesajının alınması sağlanmıştır.

Adım-4: Saldırgan, ziyaretçi görüşlerinin kaydedildiği XSS Stored modülündeki metin kutusu aracılığıyla zararlı kodun veri tabanına kaydedilmesi sağlayarak kalıcı olması sağlanmıştır. Zararlı kodu veri tabanına enjek edilmesine ait ekran görüntüsü Şekil 18'de sunulmuştur.

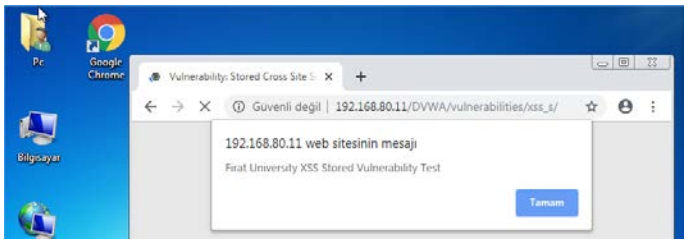


Şekil 17 Enjekte edilen zararlı kodun çalışmasına ait ekran görüntüsü



Şekil 18 Zararlı kodun ziyaretçi sayfasından veri tabanına enjekte edilmesi

Adım-5: Web uygulamasındaki ziyaretçi sayfası çalıştırıldığında veri tabanına kayıtlı ziyaretçi görüşleri veri tabanından okunarak tarayıcıya yüklenmektedir. Ziyaretçi görüşlerinin tarayıcıya yüklenmesi sırasında zararlı kodlar çalışarak kullanıcının XSS saldırısına maruz kalması sağlanmıştır. Bu adımdan sonra ziyaretçi sayfasını açan tüm kullanıcılar Şekil 19'da sunulduğu gibi XSS saldırısına maruz kalacaktır.



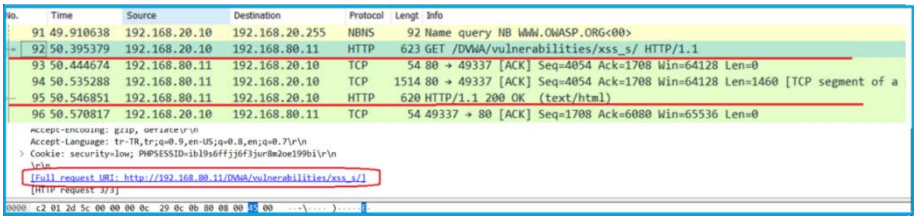
Şekil 19 Saldırıya uğrayan kullanıcı tarayıcısı

Web sitesine zararlı kod gömme yöntemi ile gerçekleştirilen saldırı sonucu web uygulamasına zararlı kodlar enjekte edilerek web uygulamasının kalıcı olarak zarar görmesi sağlanmıştır. Ayrıca saldırıya maruz kalan web uygulamasını ziyaret eden tüm kullanıcıların, enjekte edilen zararlı koddan etkilenerek tarayıcı üzerinden saldırıya açık hale gelmesi sağlanmış ve uygulama bölümünde ekran görüntüleri ile sunulmuştur.

Zararlı kodun enjekte edilmesi esnasında gerçekleşen tüm adımlara ait ağ kayıtları wireshark yazılımı ile kayıt altına alınarak ağ trafiğinde anormal herhangi bir iletişim olup olmadığı tespit edilmeye çalışılmıştır.

Ancak Şekil 20'de sunulan ağ trafiği kayıtlarından da anlaşılacağı üzere site zitaretçisi ile web uygulaması arasında herhangi bir anormal trafik tespit edilememiştir.

Saldırgan hedef uygulamaya zararlı kodu enjekte etmek için yalnızca bir defa iletişim kurmuş ve XSS Reflected ve XSS Stored yöntemlerini kullanarak zararlı kodları enjekte etmiştir.



Şekil 20 XSS saldırısı anındaki ağ trafiği

5. Ağ Saldırılarının Engellenebilmesi İçin Çözüm Yaklaşımları

Çalışma kapsamında uygulamaları gerçekleştirilen farklı saldırı tür/yöntemlerinin zararlı etkilerini en aza indirebilmesi veya tamamen engelenebilmesi için alınması gereken tedbirler/önlemlere ait çeşitli öneriler bu bölümde sunulmaktadır.

5.1. DoS/DDoS Saldırılarından Korunmak İçin Alınması Gereken Tedbirler

Bilgisayar ağlarına yapılan saldırılar göz önüne alındığında korunması en zor saldırı türü olarak DoS/DDoS saldırıları gösterilebilir. Korunmasındaki zorluklar göz önüne alındığında değişik tür ve seviyede farklı koruma önlemleri alma zorunluluğunu ortaya çıkartmaktadır.

Hizmet aksatma saldırılarından korunmanın temelinde ağ yapısının iyi tasarlanması gelmektedir. Tasarımı iyi yapılmış bir ağ'da; güvenlik duvarı, sunucular, router, switch, kablosuz erişim cihazları ve ağ'a bağlanan diğer tüm cihazların haritasının çok iyi dokümante edilmesi gerekmektedir. Ağ yöneticisinin bilgisi ve izni dışında ağ'a herhangi bir cihaz eklenemesi veya devre dışı bırakılması yapılamamalıdır. Kritik öneme sahip ağ cihazlarının fiziki olarak güvenliği sağlanarak, yetkili personelin dışındaki müdahaleye açık olmaması sağlanmalıdır[3],[4],[29].

Saldırıların yerel ağ'dan yapılabileceği düşünülerek yerel ağdaki cihazların güvence altına alınması sağlanmalıdır. Cihazlara antivirüs yazılımları yüklenmesi, pc'lerde korsan veya cracklı yazılım kullanımının önüne geçilmesi gibi ağ güvenliğini tehliyeye sokacak güvenlik zaafiyetlerinin önüne geçilmesi için gerekli tedirler alınmalıdır [29].

Yerel ağ'a bağlanacak kullanıcıların ağ hizmetlerinden faydalanabilmesi için kimlik doğrulama yöntemleri ile kimliğini doğrulamaya zorlanmalı kimliğini doğrulayamaması halinde ağ hizmetlerine bağlanamaması için gerekli önlemler alınmalıdır.

Hizmet aksatma saldırılarının amacı hedef ağ cihazlarını devre dışı bırakarak hizmetlerin kesintiye uğramasını sağlamaktır. İki farklı ağın haberleşebilmesi için etkileşime gireceği ilk ağ elemenı router'dır. Router iki veya daha fazla ağdan gelen-giden TCP/IP paketlerini üzerinden geçirdikten sonra ağ üzerindeki hedefine yönlendirir. Router bu özelliği nedeniyle DoS/DDoS saldırılarında etkilenen ilk ağ cihazıdır. Saldırı anında router devre dışı kaldığında ağ'ın diğer ağlarla bağlantısı kesilmiş olacağı için hizmetlerde kesinti yaşanmasına sebep olacaktır. Bu nedenle işletime alınacak router üzerinde üretici firma tarafından eklenen güvenlik ayarları aktif hale getirilerek önlem alınmalıdır. Kullanıcı veya ip bazında bant genişiliği üst limiti belirlenerek tüm kullanıcıların belirlenen bant genişliğinin üzerine çıkması engellenmelidir. Bant genişliği sınırlaması getirilerek belli bir sayının altındaki bağlantı sayısına ulaşan DoS/DDoS saldırıları kontrol altına alınabilecektir [30].

Router ile birlikte gelen kontrol yazılımları sayesinde, sistem kaynaklarını aşırı tüketen yerel ağ dışındaki ip adreslerini tespit edip otomatik bloklayabileceği imza ekleme mekanizması aktif hale getirilmelidir. Yerel ağdan gelen ve sistem kaynaklarını aşırı tüketen cihazlar engellenerek önleyici tedbirler devreye alınmalıdır. Daha önce DoS/DDoS saldırısı yaptığı bilinen ip adresleri tespit edilerek ACL listelerine eklenerek bağlantı talepleri otomatik rededilmelidir. Port güvenliği sağlanarak güvenilen portlar dışında kalan portlar erişime kapatılmalıdır [2].

Router ile yerel ağ arasına saldırı tespit ve önleme (IDS/IPS) sistemleri entegre ederilerek, tüm ağ trafiği kontrol altına alınmalıdır. Geçmiş yıllarda gerçekleştirilen ve kaynağı bilinen DoS/DDoS saldırılarına ait imza kuralları oluşturulup aktif hale getirilerek aynı kaynaklardan gelebilecek olası saldırılar

engellmiş olacaktır. Ayrıca ağ'a yerleştirilen IDS/IPS sayesinde ağ trafiği merkezi bir noktadan kontrol altına alındığı için tüm ağ hareketleri analiz edilerek, zararlı ağ trafiği veya bir saldırı kolayca tespit edilip gerekli tedbirler hızlıca alınabilecektir [3],[4],[5],[7].

İmza tabanlı saldırı tespit ve önleme sistemleri bilinen saldırıları yakalayıp önlemede çok etkili olabilmektedir ancak geçmişte hiç denenmemiş ve ilk defa kullanılacak bir saldırı yöntemi ile yapılacak saldırıyı tespit etmekte yetersiz kalmaktadır. Bu nedenle ağ trafiğini çevrimiçi analiz eden anomali tabanlı yeni nesil akıllı saldırı tespit sistemleri entegre edilmelidir [2],[8],[9].

5.2. SQL Enjeksiyon Saldırılarından Korunmak İçin Alınması Gereken Tedbirler

Veritabanı sunucuları ve web uygulamaları kritik öneme sahip veriler barındıran yapı veya uygulamalardır. Bu nedenle barındırdıkları verilere yetkisiz erişim sağlanması, verilerin bozulması, silinmesi, değiştirilmesi veya çalınması gibi risklerle karşı karşıya kalması kaçınılmazdır. Veri barındırıan sistemlerin SQL enjeksiyon saldırılarından korunması için alınabilecek önlemler aşağıda maddeler halinde açıklanmaya çalışılmıştır.

DB yöneticileri veritanabında işlem yaparken tam yetkili ve bilinirliği yüksek root veya admin kullanıcıları yerine yetkileri kısıtlanmış kolay tahmin edilemeyen kullanıcılar ile çalışılmalıdır. Kullanıcı adı, şifre, biometrik veri, kredi kartı gibi çok kritik verilerin tutulduğu tablo isimleri içeriğinde sakladığı veri ile ilişki kuracak şekilde seçilmemelidir [11],[12].

Web Uygulamasından veritabanına yapılacak bağlantılarda admin grubundan bir kullanıcı yerine yetkileri azaltılmış daha düşük seviyeli bir kullanıcı ile bağlanarak işlem yapılmalıdır.

Web ve veritabanı sunucusuna ait yazılımlardaki hata mesajları SQL enjeksiyon saldırılarının çıkış noktası olması nedeniyle, hata mesajlarının kapatılması güvenlik açısından önemlidir [11].

Web uygulamaları, kullanıcılardan alınacak verileri web form elemanları aracılığıyla almaktadır. Formlarda kullanılan metin kutuları ile metin ve sayısal veriler kullanıcılardan alınarak işleme tabi tutulmaktadır. SQL enjeksiyon saldırılarında kullanılan tek tırnak karakteri ('), eşittir işareti (=), ünlem işareti(!) gibi saldırılara açık kapı bıracak işaretlerin Regular Expression Validator sınıfı ile kontrol edilerek metin kutularından girişine izin verilmemelidir. Aynı şekilde saldırılarda sorgu şartlarını devre dışı bırakmak için kullanılan **"OR '1'='1'"** gibi mantıksal ifadeler içeren kelimelerin filtre edilerek temiznlendikten sonra kullanılması gerekmektedir [13].

Metin kutuları aracılığıyla kullanıcılardan bilgi alırken, verinin türü ve veritabanı tablosunda o alan için ayrılmış uzunluk değerini geçmeyecek şekilde sınırlama getirilmelidir. Örneğin kimlik numarası için veri girşi yapılacaksa 11 karekterden fazla rakamın girişine izin verilmemelidir. Bu şekilde hem olası SQL enjeksiyon saldırısının önüne geçilmiş olunur hem de veri tabanında kimlik numarası için ayrılan uzunluktan daha fazla değer girildiğinde oluşacak taşma hatalarının önüne geçmiş olunacaktır.

SQL sorgularında kullanılan select, update, insert, delete, union, order vb.. deyimlerin metin kutularına girileceği varsayılarak, metin kutusundaki veri işleme alınmadan önce yukarıda belirtilen deyimleri içerip içermediği bir fonksiyon yardımı ile kontrol edilerek temizlenmelidir [11].

Uygulamada kullanılan SQL sorguları oluşturulurken kullanıcıdan alınan girdiler her bir sorgu elemanı için ayrı ayrı parametre gönderilerek yapılmalı, tek cümleden oluşan SQL sorguları kullanılmamalıdır.

Veritabanı sunucusu, güvenlik duvarı ile koruma altına alınarak, kullanıcılardan gelen URL içerikleri önişleme tabi tutulmalıdır. URL içeriklerinde SQL enjeksiyon saldırısında kullanılacak içerik barındıran talepler ile talebin geldiği ip adresi için geçici veya daimi olarak engelleyici imzalar tanımlanmalıdır [16].

5.3. XSS Saldırılarından Korunmak İçin Alınması Gereken Tedbirler

Yazılım teknolojilerinin gelişmesine paralel olarak XSS açıkları üzerinden yapılan saldırılar daha karmaşık ve önlem alınması zor saldırı yöntemlerine dönüşmüştür. Ancak saldırı karmaşıklığı ve yöntemleri geliştikçe saldırılardan korunmak için yeni yöntem ve çözüm yollarıda gelişmektedir.

Makale kapsamında gerçekleştirilen XSS saldırısı ve saldırganların en sık kullandığı XSS ataklarından korunmak için alınması gereken önlemler aşağıda sunulmuştur.

Dinamik web uygulaması geliştirilirken uygulamayı kullanacak tüm kullanıcıları potansiyel saldırgan olarak kabul edip, bu varsayım üzerine güvenli uygulama geliştirme yöntemlerine göre uygulama geliştirilmelidir. Dinamik web uygulamaları; Kullanıcı ile uygulama arasındaki bilgi alış verişini web form elemanları aracılığıyla gerçekleştirir. Web form elemanı olarak kullanılan metin kutuları zararlı kod filtresinden geçirilmeden kullanıması halinde XSS saldırılarına açık kapı bırakacaktır. Bu nedenle metin kutularından alınan girdi değerleri filtre işlemine tabi tutularak içeriğinde XSS saldırısına yol açacak deyim ve kodlar temizlendikten sonra kullanılmalı veya içeriğin uygun olmadığı kullanıcıya mesaj ile bildirilerek girişi yapılan metin iptal edilmelidir. Örneğin içerğinde **<script>alert(“Firat University XSS Vulnerability Test”)</script>** şeklinde JS kodları olan bir girdi değeri filtre edilerek,"<script>, alert, </script>" vb. içerik temizlendikten sonra işleme alınmalıdır [14],[16].

Metin kutuları ile kullanıcıdan bilgi alınırken, alınacak bilginin veri tipine uygun kısıtlamalar getirilmelidir. Örneğin tarih formatında bir veri alınacaksa metin kutusuna rakam, nokta(.) veya "/" karekterinden başka karakter girişine izin verilmemelidir.

Saldırganların metin kutusuna **<script>alert('XSS Test')</script>** şeklinde XSS saldırısı gerçekleştirebilecek zararlı kod girişi yapabilir. Saldırganın bu kodları enjekte edeceği düşünülerek metin kutusu içeriğindeki kaçış karakterleri replace fonksiyonu ile değiştirilmedilir. Örneğin < ve > karakterleri < ve > karakterleri ile değiştirilmelidir. Böylece ekrana metin kutusuna girişi yapılan bilgi gelecektir ancak bir JS kodu olarak çalışmayacaktır. Kaçış karakterlerine ait örnekler Tablo 4’de verilmiştir.

Tablo 4 Kaçış karakterleri tablosu

Çıktı	Numerik Kod	Hex Kod
(	&#40;	&#x28;
)	&#41;	&#x29;
<	&#60;	&#x3C;
>	&#62;	&#x3E;

Kullanıcı girdi değerlerinden hangi deyim, komut veya karakterlerin kabul edileceği hangilerinin kabul edilmeyeceği önceden tanımlanan white ve black listeler aracılığı ile kontrol altına alınmalıdır [31].

URL istekleri işleme alınmadan önce içeriğine JS kodlarının yerleştirilip yerleştirilmediği uygulama içerisinde kontrol edilmeli ve filtreden geçirildikten sonra işleme alınmalıdır. Tarayıcıdan http://192.168.80.11/XSSTest/Liste.php?Id=<script>alert('XSS Test')</script> şeklinde yapılan bir istek filtre edilmeden direk kullanılırsa ekrana 'XSS Test' şeklinde mesaj verecektir.

URL istekleri web sunucusuna iletilmeden önce güvenlik duvarı URL filtresi ile kontrolden geçirilmeli ve XSS saldırısına sebep olacak bağlantı talepleri red edilmelidir [16].

5.4. Siber Saldırılardan Korunmak İçin Alınması Gereken Güvenlik Politikalarına Ait Öneriler

Kritik sistemlerde çalışan personele siber güvenlik ve farkındalık temalı eğitim, konferans ve bilgilendirmeler düzenli aralıklarla verilerek, personelin siber saldırılara karşı farkındalığının açık olmasını sağlayacı planlama yapılmalıdır.

Ağ'larda kullanılan cihazlarda koşturulan yazılımlar ile ağ’da çalışan uygulamaların, yazılım üreticilerinden güvenlik açıklarını gidermeye yönelik güncelleme paketlerini en kısa sürede sisteme entegre edecek alt yapı güncelleme sistemleri hayata geçirilmelidir.

Tüm ağ, belirli periyotlarla penetrasyon testlerine tabi tutularak, tespit edilen açıklar en hızlı şekilde kapatılmalıdır.

Yüksek riskli ve güvenlik açıklarının sıklıkla istismar edildiği IoT sistemleri, kritik öneme sahip sistemlerden izole edilerek kritik sistemler silahsızlandırılmış DMZ alanlarında konumlandırılmalıdır [23].

Kullanıcıların ağ hizmetlerinden faydalanabilmesi için kimlik doğrulama sistemleri üzerinden kimliğini doğrulayarak ağ hizmetlerine erişim izni verilmelidir. Kimlik doğrulama yapamayan kullanıcıların talepleri red edilerek erişim talebi engellenmelidir.

Yerel kullanıcılarının İnternet üzerinden gerçekleştireceği iletişimin üçüncü taraflarca ele geçirilebileceği düşünülerek verilerin şifreli gönderilip alınabilmesi için SSL sertifikaları kullanılmalıdır.

Ağ dışından yerel ağ'a yapılacak bağlantıların VPN(Sanal Özel Ağ) alt yapısı ile yapılabilecek şekilde tasarlanarak güvenli bağlantı ortamı sağlanmalıdır.

Ağ tasarımı yapılırken farklı vlan'lar tanımlanmalı ve ağ'daki cihazların kontrolsüz bir şekilde birbirleri ile haberleşmesi engellenmelidir.

Ağ trafiği ve kullanıcı hareketleri log'lanarak elektronik imza ile imzalanmalı ve resmi kayıt haline getirilmelidir [29].

6. Sonuçlar

Bilgisayar korsanları tarafından en sık kullanılan ve yıkım gücü en yüksek olan saldırı teknikleri kullanılarak gerçekleştirilen saldırıların gerçek bir ağ'da hangi hasarlara yol açabileceği GNS3 platformunda uygulamalı olarak incelenmiştir. Saldırılar sırasında saldırganın ağ'da bıraktığı izlerin tespit edilip edilemeyeceğinin mümkün olup olmadığı uygulamalı olarak ele alınmıştır.

DDoS saldırısı uygulaması ile güvenlik duvarı ile izole edilmiş DMZ ağ alanına 2 farklı saldırı gerçekleştirilerek web sunucusu ve güvenlik duvarının saldırı anındaki davranışları wireshark ile kayıt altına alınmıştır. Saldırı sonrası web sunucusun hizmet aksatması sağlanarak devre dışı kalması başarılmıştır. DDoS saldırısına ait ağ trafiği incelenerek saldırganın ip adresi, hedef ip adresi, saldırıda kullanılan protokol ve saldırı paket boyutları açıkça tespit edilmiştir.

SQL enjeksiyon saldırısı ile DMZ alanında hizmet veren web uygulamasına saldırı gerçekleştirilerek veri tabanında kayıtlı kullanıcı adı ve şifre özetleri ele geçirilmiştir. SQL enjeksiyon saldırısına ait tüm adımlar açıklanarak, saldırı anındaki ağ trafiği wireshark yazılımı ile kayıt altına alınmıştır. Kayıt altına alınan ağ paketlerin incelenerek saldırıya ait SQL enjeksiyon kodları tespit edilmiştir.

XSS saldırısı ile tasarlanan kampüs ağındaki 2 farklı network arasında 2 farklı XSS saldırısı senaryosu gerçekleştirilerek web uygulaması ve site ziyaretçisi saldırıya maruz bırakılmıştır. Yapılan saldırıya ait ağ kayıtları wireshark yazılımı ile kayıt altına alına XSS saldırısı tespit edilmiştir.

Her 3 saldırı yöntemi ile 5 farklı saldırı gerçekleştirilmiş ve saldırı anındaki ağ kayıtları Wireshark ile incelenmiştir. Yapılan incelemede; DDoS ve SQL enjeksiyon saldırısı esnasında saldırgan ile kurban arasındaki zararlı trafik ve komutlar tespit edilmiştir. Elde edilen kayıtlardan yola çıkarak; Yerel ağ paketlerini anlık olarak inceleyerek, çeşitli DDoS saldırı algoritmaları ile imza tabanlı saldırı tespit sistemlerini birlikte çalıştıran karma saldırı tespit sistemi geliştirilebilecektir.

Web uygulaması geliştiricilerinin kodlama hatalarından kaynaklanan SQL enjeksiyon açıkları, geliştirilecek yeni nesil saldırı tespit sistemi tarafından tespit edilerek saldırılardan korunacaktır. Saldırganın web uygulamasına yaptığı isteklere ait URL içerikleri, anlık olarak incelenip SQL enjeksiyon saldırılarında kullanılan içerikler taşıdığı tespit edilen URL istekleri işleme alınmadan engellenebilecektir.

XSS saldırısına ait ağ kayıtları incelendiğinde kurban pc ile zararlı web sitesi arasında istek-cevap şeklinde gelişen normal ağ trafiği oluştuğu, anormal herhangi bir ağ trafiğinin oluşmadığı gözlemlenmiştir. Ancak web sunucusunu kendi bünyesinde barındıran ağ yapılarında, web uygulamasındaki XSS açıkaları üzerinden XSS saldırıları gerçekleştirilebilir. Web uygulamasındaki kodlama hatalarından kaynaklanan bu açıklardan gelebilecek XSS saldırıları geliştirilecek yeni nesil

saldırı tespit sistemleri ile tespit edilip silinebilecektir. SQL enjeksiyon saldırılarını tespit etmekte kullanılan yöntem XSS saldırı tespit yöntemi olarak da kullanılabilecektir.

Ağ saldırılarının uygulamalı olarak incelendiği çalışmamızı diğer çalışmalardan ayıran, 3 farklı ağ saldırısının 5 farklı saldırı yöntemi ile birlikte ele alınmış olmasıdır. Literatürdeki çalışmalara bakıldığında ağ saldırılarının bireysel olarak incelendiği ve farklı saldırı yöntemlerinin bir arada uygulanmadığı görülmüştür. Ayrıca GNS3 platformunda gerçekleştirilen çalışmalar incelendiğinde ağırlıklı olarak ağ uygulama protokollerinin performansına yönelik çalışmalar yapıldığı görülmektedir. Bu ise ağ saldırılarının incelenmesine yönelik yapmış olduğumuz çalışmayı diğer çalışmalardan farklı kılmaktadır.

Referanslar

[1] "Cyber crime attacks experienced by global companies 2017", Statista. [Çevrimiçi]. Erişim adresi: https://www.statista.com/statistics/474937/cyber-crime-attacks-experienced-by-global-companies/. [Erişim: 20-Ara-2019].

[2] "Snort - Network Intrusion Detection & Prevention System". [Çevrimiçi]. Erişim adresi: https://www.snort.org/. [Erişim: 14-Oca-2020].

[3] N. Goksel ve M. Demirci, "DoS Attack Detection using Packet Statistics in SDN", *in 2019 International Symposium on Networks, Computers and Communications (ISNCC)*, ss. 1-6, 2019, doi: 10.1109/ISNCC.2019.8909114.

[4] Ş. Sağiroğlu, E. Yolaçan, ve U. Yavanoğlu, "Zeki saldırı tespit sistemi tasarımı ve gerçekleştirilmesi", *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, c. 26, sy 2, 325-340, 2011

[5] I. Karadoğan ve R. Daş, "Analysis of attack types on TCP/IP based networks via exploiting protocols", *in 2015 23nd Signal Processing and Communications Applications Conference (SIU), Inonu University*, Malatya, ss. 1785-1788, 2015, doi: 10.1109/SIU.2015.7130200.

[6] "Scapy". [Çevrimiçi]. Erişim adresi: https://scapy.net/. [Erişim: 18-Ara-2019].

[7] R. Das ve G. Tuna, "Packet tracing and analysis of network cameras with Wireshark", *in 2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, Romanya, ss. 1-6, 2017, doi: 10.1109/ISDFS.2017.7916510.

[8] R. Abdulhammed, M. Faezipour, H. Musafer, ve A. Abuzneid, "Efficient Network Intrusion Detection Using PCA-Based Dimensionality Reduction of Features", *in 2019 International Symposium on Networks, Computers and Communications (ISNCC)*, ss. 1-6, 2019, doi: 10.1109/ISNCC.2019.8909140.

[9] T. Tuncer ve Y. Tatar, "Fpga Tabanlı Programlanabilir Gömülü Saldırı Tespit Sisteminin Gerçekleştirilmesi", *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi 27*, sy 1, 2013.

[10] J. J. Shah ve D. L. G. Malik, "Impact of DDOS Attacks on Cloud Environment", *International Journal of Research in Computer and Communication Technology*, Vol 2, Issue 7, Tem.-2013

[11] P. Kumar ve R. K. Pateriya, "A survey on SQL injection attacks, detection and prevention techniques", in 2012 Third International Conference on Computing, *Communication and Networking Technologies (ICCCNT'12)*, Coimbatore, ss. 1-5, 2012, doi: 10.1109/ICCCNT.2012.6396096.

[12] D. Demirol, R. Daş, ve M. Baykara, "SQL enjeksiyon saldırı uygulaması ve güvenlik önerileri", *in 1st International Symposium on Digital Forensics and Security (ISDFS'13)*, Elazığ, ss. 62-66, 2013.

[13] A. Al-Mahrouqi, P. Tobin, S. Abdalla, ve T. Kechadi, "Simulating SQL-Injection Cyber-Attacks Using GNS3", *International Journal of Computer Theory and Engineering*, c. 8, ss. 213-217, Haz. 2016, doi: 10.7763/IJCTE.2016.V8.1046.

[14] M. Baykara ve S. Guclu, "Applications for detecting XSS attacks on different web platforms", *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* ss. 1-6, 2018, doi: 10.1109/ISDFS.2018.8355367.

[15] S. Djanali, F. X. Arunanto, B. A. Pratomo, A. Baihaqi, H. Studiawan, ve A. M. Shiddiqi, "Aggressive web application honeypot for exposing attacker's identity", *in 2014 The 1st International Conference on Information Technology, Computer and Electrical Engineering*, ss. 212-216, 2014, doi: 10.1109/ICITACEE.2014.7065744.

[16] T. Gunawan, M. K. Lim, M. Kartiwi, N. A. Malik, ve N. Ismail, "Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks", *Indonesian Journal of Electrical Engineering and Computer Science*, c. 12, ss. 729-737, Kas. 2018, doi: 10.11591/ijeecs.v12.i2.pp729-737.

[17] H. Sabrine, B. Abderrahmane, ve S. Fouzi, "Comparative Study of Security Methods against DDOS Attacks in Cloud Computing Environment", içinde *2019 International Symposium on Networks, Computers and Communications (ISNCC)*, Haz. 2019, ss. 1-5, doi: 10.1109/ISNCC.2019.8909110.

[18] "OWASP Top Ten Web Application Security Risks | OWASP". https://owasp.org/www-project-top-ten/ (Erişim Haz. 17, 2020).

[19] "Database SQL Reference". [Çevrimiçi]. Erişim adresi: https://docs.oracle.com/cd/B19306_01/server.102/b14200/intro001.htm. [Erişim: 17-Ara-2019].

[20] "CWE - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (4.0)". https://cwe.mitre.org/data/definitions/77.html (Erişim Haz. 17, 2020).

[21] H. Alnabulsi, R. Islam, ve M. Talukder, "GMSA: Gathering Multiple Signatures Approach to Defend Against Code Injection Attacks", *IEEE Access*, c. 6, ss. 77829-77840, 2018, doi: 10.1109/ACCESS.2018.2884201.

[22] V. Clincy ve H. Shahriar, "Web service injection attack detection", içinde *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, ss. 173-178, Ara. 2017, doi: 10.23919/ICITST.2017.8356371.

[23] H. Bağci, "Sosyal Mühendislik ve Denetim", *Denetişim*, sy 1, ss. 42-51, Tem. 2016.

[24] M. Baykara ve R. Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems", *Journal of Information Security and Applications*, c. 41, ss. 103-116, Ağu. 2018, doi: 10.1016/j.jisa.2018.06.004.

[25] M. Baykara ve R. Daş, "A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems", *International Journal of Computer Networks and Applications*, c. 2, sy 5, s. 9, 2015.

[26] M. Baykara ve R. Daş, "SoftSwitch: a centralized honeypot-based security approach using software-defined switching for secure management of VLAN networks", *Turk J Elec Eng & Comp Sci (2019) 27: 3309 – 3325 © TÜBİTAK doi:10.3906/elk-1812-86* s. 17.

[27] "GNS3, 27-Ara-2019. [Çevrimiçi]. Erişim adresi: https://docs.gns3.com [Erişim: 27-Ara-2019].

[28] DVWA - Damn Vulnerable Web Application, "DVWA - Damn Vulnerable Web Application". Erişim adresi: http://www.dvwa.co.uk/. [Erişim: 02-Oca-2020].

[29] D. Ş. Sağiroğlu ve D. M. Alkan, "Siber güvenlik ve Savunma Farkındalık ve Caydırıcılık", s. 402.

[30] "Cisco Router Security Solutions - Technical Overview", https://www.cisco.com/c/dam/en/us/products/collateral/security/router-security/routersec_tdm.pdf s. 116. [Erişim: 16-May-2020].

[31] I. Yusof ve A.-S. K. Pathan, "Preventing persistent Cross-Site Scripting (XSS) attack by applying pattern filtering approach", içinde *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, ss. 1-6, Kas. 2014, doi: 10.1109/ICT4M.2014.7020628.