T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

VOIP SİSTEMLERİNDE SIZMA TESTLERİ ile GÜVENLİK ANALİZİ

Kübra SENCAR

DANIŞMAN
Prof. Dr. Ahmet SERTBAŞ

II. DANIŞMAN
Doç. Dr. Muhammed Ali AYDIN

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

İSTANBUL-2019

Uygundur
15.01.2020

Prof. Dr. Ahmet SERTBAŞ
Bilgisayar Mühendisliği
Bölüm Başkanı

Bu çalışma 16.12.2019 Tarihinde aşağıdaki jüri tarafından Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı Yüksek Lisans Tezi olarak kabul edilmiştir.

TEZ JÜRİSİ

Prof. Dr. Ahmet SERTBAŞ
İstanbul Üniversitesi-Cerrahpaşa
Fakültesi

Dr.Öğr.Üyesi Özgür Can TURNA
İstanbul Üniversitesi-Cerrahpaşa
Fakültesi

Dr.Öğr.Üyesi Zeynep TURGUT
Haliç Üniversitesi -
Mühendislik Fakültesi

20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi-Cerrahpaşa'nın abonesi olduğu intihal yazılım programı kullanılarak Lisansüstü Eğitim Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Bu çalışma, İstanbul Üniversitesi Cerrahpaşa Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans kapsamında hazırlanan "VoIP Sistemlerinde Sızma Testleri ile Güvenlik Analizi" başlıklı yüksek lisans tez çalışmasını içermektedir.

Tez çalışmam ve eğitimim boyunca bana yol gösteren, desteğini ve ilgisini esirgemeyen, değerli görüşlerini benimle paylaşan, bana her konuda öncülük eden danışman hocalarım Sayın Prof. Dr. Ahmet SERTBAŞ'a ve Sayın Doç. Dr. Muhammed Ali AYDIN'a sonsuz teşekkürlerimi sunarım.

Bu çalışmayı hazırlarken geçirdiğim süreçte bilgi ve deneyimleri ile bana yol gösteren ve yardımını esirgemeyen Sayın Araş. Gör. Dr. M. Erdem İSENKUL'a teşekkürlerimi sunarım.

Tezimin yazım aşamasında her türlü maddi manevi desteklerini, yardımlarını esirgemeyen canım kadar çok sevdiğim arkadaşlarıma ve Oğuz ŞAHİN'e teşekkürlerimi sunarım.

Hayatım boyunca maddi manevi desteklerini benden esirgemeyen, verdikleri sevgiyle beni hayata bağlayan annem, babam, ablalarım ve Damla'ma binlerce kez teşekkür ederim.

Aralık 2019 Kübra SENCAR

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Kısaltmalar	Açıklama
3DES	: Triple-DES
ACK	: Acknowledgement
AES	: Advanced Encryption System
AH	: Authentication Header
ARP	: Address Resolution Protocol
CPU	: Central Processing Unit
DES	: Data Encryption Standard
DHCP	: Dynamic Host Configuration Protocol
DDoS	: Distributed Denial of Service
DNS	: Domain Name System
DoS	: Denial of Service
ESP	: Encapsulating Security Payload
FTP	: File Transfer Protocol
HTTP	: Hyper Text Trasfer Protocol
ICMP	: Internet Control Message Protocol
IDS	: Intrusion Detection System
IEEE	: Institute of Electrical and Electronics Engineers
IETF	: Internet Engineering Task Force
IP	: Internet Protocol
IPS	: Intrusion Prevention System
IPSec	: Internet Protocol Security
ITU	: International Telecomunication Union
LAN	: Local Area Network
MAC	: Media Access Control
MGCP	: Media Gateway Control Protocol
MITM	: Man In The Middle
OSI	: Open System Interconnection
PBX	: Public Branch Exchange
PSTN	: Public Switched Telephone Network
QoS	: Quality of Service

RAM : Random Access Memory
RFC : Request for Comments
RSA : Rivest Shamir Adleman
RTCP : Real-time Transport Control Protocol
RTP : Real-time Transport Protocol
SDP : Session Description Protocol
SIP : Session Initiation Proocol
SMTP : Simple Mail Transfer Protocol
SPAM : Unsolicted Email
SPIT : Spam over Internet Telephony
SRTP : Secure Real-time Transport Protocol
SSH : Secure Shell
SYN : Synchorize
TCP : Transmission Control Protocol
TLS : Transport Layer Security
ToS : Terms of Service
UA : User Agent
UAC : User Agent Client
UAS : User Agent Server
UDP : User Datagram Protocol
URI : Uniform Resource Identifier
VoIP : Voice over Internet Protocol

ÖZET

YÜKSEK LİSANS TEZİ

VOIP SİSTEMLERİNDE SIZMA TESTLERİ ile GÜVENLİK ANALİZİ

Kübra SENCAR

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman : Prof. Dr. Ahmet SERTBAŞ

II. Danışman : Doç. Dr. Muhammed Ali AYDIN

VoIP, ses paketlerinin internet üzerinden iletilmesini sağlayan bir teknolojidir. VoIP'nin, SIP teknolojisiyle beraber kullanılmaya başlanması ile VoIP teknolojisi, yeni nesil telekom dünyasında popüler hale gelmeye başlamıştır. Bu popülerliğin ve kullanım oranlarının son yıllarda artması ile VoIP/SIP teknolojilerinde güvenlik sorunları ile karşılaşılmaya başlanmıştır.

VoIP teknolojisinde iletim, IP ağı üzerinden gerçekleştiği için internette oluşan bütün sorunlar ve güvenlik tehditleri bu teknoloji için de geçerli olmaktadır. Sistemde tehdit hedefi olabilecek unsurlar; kullanılan protokoller, VoIP istemci ve sunucu bileşenleri, ağda yer alan diğer sistemler ile etkileşimini sağlayan çeşitli yazılımlar gibi farklı parametrelerden oluşabilmektedir. Bunların sonucunda VoIP trafiği kötü niyetli kişiler tarafından ele geçirilebilir, kopyalanabilir, değiştirilebilir ya da engellenebilir.

Bu tez çalışması ile bu sıkıntılara istinaden hem bireysel hem de kurumsal kullanıcılar için popüler hale gelen VoIP mimarisi incelenmiştir. VoIP güvenliğinin proaktif yaklaşım ile değerlendirilmesi için VoIP sistemlerinde sızma testi konusu ve etkin güvenlik önlemleri ele alınmıştır. Ek olarak, gerçek bir VoIP güvenlik laboratuvar ortamı kurularak, VoIP sistemlerine yönelik DoS/DDoS saldırıları düzenlenmiş ve sistemlerin bu tür saldırılara karşı duyarlılıkları ölçümlenmiştir. Elde edilen çıktılar yardımıyla VoIP sistemleri için bu tür saldırılara karşı

güvenlik iyileştirmeleri amacıyla fikir verilmesi ve bu iyileştirmelerin, güvenlik tavsiyeleri olarak önerilmesi amaçlanmıştır.

Aralık 2019, 79 sayfa.

Anahtar kelimeler: VoIP, VoIP güvenliği, DoS saldırıları, Flood tabanlı DoS saldırıları, Güvenlik politikaları.

SUMMARY

M.Sc. THESIS

SECURITY ANALYSIS with PENETRATION TEST OVER VOIP SYSTEMS

Kübra SENCAR

Istanbul University-Cerrahpasa

Institute of Graduate Studies

Department of Computer Engineering

Supervisor : Prof. Dr. Ahmet SERTBAŞ

Co-Supervisor : Assoc. Prof. Dr. Muhammed Ali AYDIN

VoIP is a technology allowing voice packets to be transmitted over the Internet. VoIP technology, together with the use of SIP technology, has started to become more popular in the new generation telecom world. In recently years, with the increasing popularity and usage rates, have started to be faced with security problems in VoIP/SIP technology.

All issues and security threats on internet are valid for the VoIP technology since the transmission occurs over the IP network. The possible threat parameters on the VoIP system may consist of different parameters like used protocol, VoIP client and server components, various software forming an interaction with other systems in the network. As a result of these, VoIP traffic can be captured, copied, changed or blocked by attacker.

In this thesis, the VoIP technology architecture that recently popularizes for both individual and enterprise users are examined based on the aforementioned issues. In order to evaluate the security of VoIP with proactive approach, the subject of VoIP penetration tests and active security precautions are processed. In addition to this, by establishing a real VoIP security test laboratory conditions for DoS/DDoS attacks on the VoIP systems and the susceptibility of VoIP systems are examined towards the aforementioned attacks. Thanks to the results, the idea for

security improvement of VoIP systems towards the attacks is given and it is suggested as a security advice.

December 2019, 79. pages.

Keywords: VoIP, VoIP security, DoS attacks, Flood based DoS attacks, Security policies.

1. GİRİŞ

VoIP, ses paketlerinin internet ağı üzerinden gerçek zamanlı olarak iletilmesini sağlayan bir teknolojidir. Bu teknolojide iletim, IP ağı üzerinden gerçekleştiği için kullanıcılar internete ulaşılabilen her noktada, VoIP teknolojisinden yararlanma imkanına sahiptirler. VoIP ile kullanıcılara, geleneksel telefon ağlarına göre daha düşük maliyetli, daha hızlı ve daha iyi bir hizmet kalitesi sağlanmaktadır. VoIP mimarisi sağladığı bu avantajlar ile yeni nesil telekom dünyasında hem bireysel hem de kurumsal kullanıcılar tarafından yaygın olarak kullanılmaya başlanmıştır.

VoIP mimarisi temelinde birçok protokolü barındırmaktadır. IP üzerinden çoklu ortam görüşmeleri gerçekleştirebilmek için geliştirilen SIP standardı, VoIP teknolojisinde sinyalleşme ve kontrol için en çok tercih edilen protokollerin başında gelmektedir.

VoIP ve SIP teknolojilerinin beraber kullanılmaya başlanması ve her geçen gün popülerliklerinin artması ile VoIP/SIP teknolojilerinde güvenlik sorunları ile karşılaşılmaya başlanmıştır. Bu teknolojide ses, görüntü ve video gibi çoklu ortam verilerinin iletimi internet üzerinden sağlanmaktadır. Günümüzde internet güvenliği tam anlamıyla sağlanamadığı için internet üzerinde oluşabilecek tüm sorunlar ve güvenlik tehditleri VoIP teknolojisi için de geçerli olmaktadır. Bu nedenlerden dolayı mevcut VoIP/SIP güvenlik teknolojileri için araştırma ve geliştirme çalışmaları önem kazanmaktadır.

Haberleşme teknolojilerinin IP dünyası ile hızla yakınsanması sonucu yaşanan en önemli problemlerden biri, VoIP sistemlerini güvenlik bakış açısı ile değerlendirip gerekli konuşlandırmaları gerçekleştirebilecek ve güvenlik yöntemi sağlayabilecek uzmanların yetersiz sayıda oluşudur. Mevcut güvenlik uzmanları bazı durumlarda, VoIP sistemleri üzerinde yeterli düzeyde güvenlik bakış açısına sahip olmayabilir ve yetersiz kalabilir. Bu nedenlerden dolayı hem ticari hem de akademik anlamda nitelikli güvenlik uzmanlarının yetiştirilmesi oldukça önemli hale gelmektedir.

Bu tez çalışması kapsamında, VoIP sistemlerine yönelik flood tabanlı DoS ve DDoS saldırı yaklaşımları geliştirilmiş, saldırı sonuçları incelenmiş ve bu tarz saldırıları önleyebilmek için güvenlik tavsiyeleri verilmiştir.

“Genel Kısımlar” bölümünde, literatür taraması kapsamında VoIP mimari yapısı, SIP protokol yapısı, VoIP/SIP sistemlerine yönelik güvenlik tehditleri ve saldırıları, VoIP/SIP güvenlik önlemleri ele alınmıştır.

“Malzeme ve Yöntemler” bölümünde, VoIP/SIP güvenliği laboratuvar ortamı oluşturulmuştur. Laboratuvar ortamında kullanılan yazılımlar ve uygulamalar ele alınmıştır. Laboratuvar ortamında, VoIP/SIP sistemlerini hedef alan flood tabanlı DoS ve DDoS saldırı senaryoları gerçekleştirilmiştir.

“Bulgular” bölümünde, flood tabanlı DoS ve DDoS saldırılarının VoIP/SIP sistemleri üzerindeki etkilerinden bahsedilmiştir ve aynı zamanda bu saldırılar sonucunda tüketilen sistem kaynaklarının istatistiksel sonuçları verilmiştir.

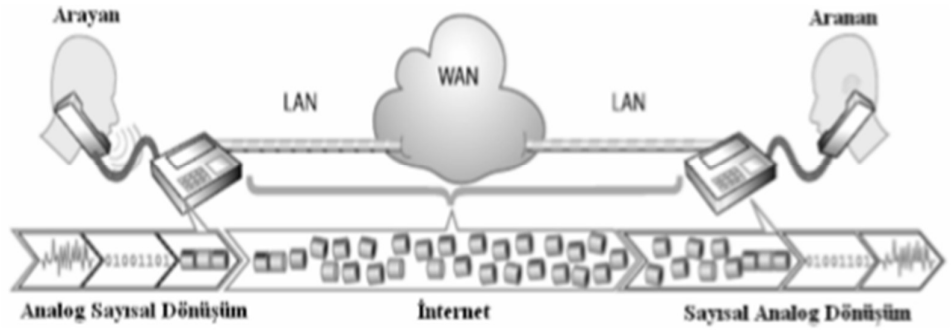
Son olarak “Tartışma ve Sonuç” bölümünde, elde edilen bulgular dikkate alınarak ve literatürdeki diğer çalışmalar göz önünde bulundurularak, VoIP sistemleri için güvenlik iyileştirmeleri sunulmuştur.

2. GENEL KISIMLAR

2.1.VOIP MİMARİSİ

Protokol, iki ya da daha fazla bilgisayar arasında iletişim kurulmasını sağlamak amacıyla tanımlanan ve standart olarak kabul edilen kurallar bütünüdür. Günümüzde çeşitli amaçlar için tanımlanan birçok protokol bulunmaktadır.

Voice over Internet Protocol (VoIP, İnternet Protokol üzerinden Ses), Internet Protocol (IP, Internet Protokolü) ağı üzerinden ses, video ve anlık mesajlaşma gibi çoklu ortam verilerinin gerçek zamanlı olarak iletilmesini sağlayan bir teknolojidir. Bu teknoloji ile herhangi bir kaynaktan elde edilen analog ses sinyalleri dijital ses sinyallerine dönüştürülerek, sıkıştırılmış küçük veri paketleri haline getirilmektedir. Elde edilen veri paketleri internet üzerinden ilgili ilgili sisteme ya da kullanıcıya gerçek zamanlı olarak iletilip, tekrar analog ses sinyallerine dönüştürülmektedir [1,2].



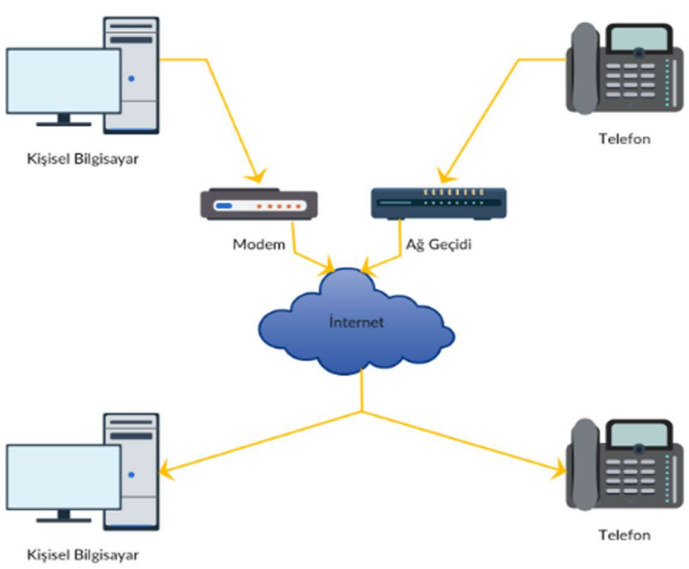
Şekil 2.1: VoIP iletişimin aşamaları [3].

VoIP mimarisi, en basit hali ile telefon görüşmelerinin geleneksel telefon ağları yerine IP tabanlı ağlar üzerinden yapılmasını sağlayan teknoloji olarak tanımlanabilir. Geleneksel telefon ağlarında iletişim kurmak isteyen iki kullanıcı arasında anahtarlama cihazları yardımı ile kapalı bir devre kurulur ve yapılacak görüşme için bir hat ayrılır. Bu hattın veri iletişimi olmadığı durumlarda bile kullanılması ve aynı hat üzerinden başka bir görüşme yapılmasına imkân sağlanmaması, geleneksel telefon ağlarının eksik kaldığı noktaların başında gelmektedir. VoIP teknolojisi ile birlikte, veri iletimi sırasında kullanıcılar arasındaki bağlantının sürekli olma zorunluluğu ortadan kaldırılmış ve kullanıcılara başka bağlantılar kurabilme imkânı da

sağlanmıştır. Bu sayede hem bant genişliğinin daha verimli bir şekilde kullanılması hem de kullanıcıların daha uygun maliyetli bir haberleşme teknolojisini kullanabilmeleri sağlanmıştır.

VoIP teknolojisinde iletim, IP ağı üzerinden gerçekleştiği için kullanıcılar, internete erişilebilen her yerde bu teknolojiden yararlanma imkanına sahiptirler. İnternete erişebilen kullanıcılar arasında kurulabilecek iletişim senaryoları şu şekilde sıralanabilir:

- Standart telefon kullanıcıları arasındaki iletişim senaryosunda, kullanıcılar bir ağ geçidi (gateway) yardımıyla IP ağına bağlanmaktadırlar.
- Standart telefon kullanıcıları ve kişisel bilgisayar kullanıcıları arasındaki iletişim senaryosunda, standart telefon kullanıcıları bir ağ geçidi yardımıyla IP ağına bağlanırken, kişisel bilgisayar kullanıcıları kullandıkları yazılımsal telefonlar ile IP ağına bağlanmaktadırlar.
- Kişisel bilgisayar kullanıcıları arasındaki iletişim senaryosunda, kullanıcılar kullandıkları yazılımsal telefonlar yardımıyla IP ağına bağlanmaktadırlar.



Şekil 2.2: VoIP iletişim senaryoları.

VoIP teknolojisi, geleneksel telefon ağları ile karşılaştırıldığında; daha düşük maliyetli ve daha hızlı bir iletişim imkânı sağlamakta ve daha iyi bir hizmet kalitesi sunmaktadır. Ek olarak yeni servislerin ve uygulamaların eklenme kolaylığı ile yeni nesil telekom dünyasında hem bireysel hem de kurumsal kullanıcılar arasında popüler hale gelmiştir. Yeni nesil telekom dünyasının

kullanıcıları arasında popüler hale gelen VoIP teknolojisinin sağladığı avantajlar şu şekilde sıralanabilir:

- İletişim yatırım maliyetlerini düşürmesi.
- Mevcut internet altyapısı üzerine kurulabilmesi.
- İnternet altyapısı olan her yerden kolayca erişilebiliyor olması.
- Yeni servislerin ve uygulamaların kolayca eklenebilmesi.
- Ses, video ve veri iletişiminin tümleşik olarak sağlanması.

VoIP mimarisi temelinde birçok protokolü barındırmaktadır. Bu mimaride, IP ağı üzerinden ses verisinin kullanıcılar arasında iletilmesi sırasında ağ iletim protokolleri, medya iletim protokolleri ve sinyalleşme protokolleri kullanılmaktadır. Bir VoIP iletişimi sırasında kullanılacak olan ağ iletim protokolü ve medya iletim protokolü VoIP sinyalleşme protokolüne bağlı olarak değişiklik göstermektedir [2,3].

Tablo 2.1: VoIP mimarisi protokolleri.

Sinyalleşme Protokolleri (H.323, MGCP, SIP)
Medya İletim Protokolleri (RTP, RTCP)
Ağ İletim Protokolleri (IP, TCP, UDP)

2.1.1. Internet Protocol (IP, Internet Protokolü)

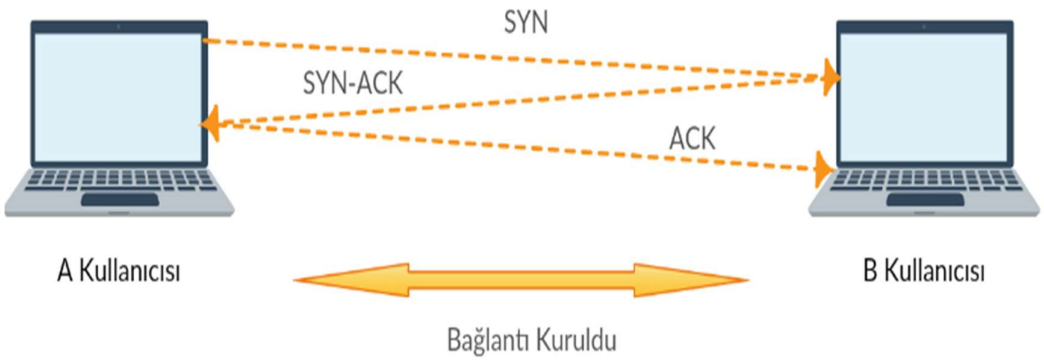
Internet protokolü, verilerin paketler halinde ilgili ağ adreslerine yönlendirilmesini sağlayan protokoldür. IP protokolü, Open System Interconnection (OSI, Açık Sistemler Bağlantısı) referans modelinin üçüncü katmanı olan ağ katmanında kullanılmaktadır. Ağ katmanı, gelen verilerin ilgili adrese yönlendirilmesini sağlamaktadır. Bu yönlendirme esnasında, gelen veri paketinin içeriği ile ilgilenilmez, sadece veri paketinin ilgili adrese iletilmesi için bir yol bulması sağlanır. İlgili yol belirlendikten sonra yönlendirme için gerekli IP başlığı, veri paketine eklenir. Eklenen IP başlığı içerisinde göndericinin internet adresi, alıcının internet adresi, protokol numarası ve sağlama toplama bilgileri yer almaktadır. IP başlığı içerisinde yer alan bu bilgiler sayesinde veri paketi “datagram” şeklinde ağda yönlendirilir [5].

2.1.2. Transmission Control Protocol (TCP, İletim Kontrol Protokolü)

İletim kontrol protokolü, OSI referans modelinin dördüncü katmanı olan taşıma katmanında kullanılmaktadır. TCP protokolü ile verinin denetimli, kayıpsız ve doğru bir şekilde iletilmesi sağlanmaktadır. Verinin denetimli ve kayıpsız bir şekilde iletilebilmesi için acknowledgement (ACK, onay) mesajları gönderilmesi sağlanır. Alıcı tarafından ilgili veri paketi için bir onay mesajı gönderilmediği takdirde, o veri paketinin alıcıya iletilmediği belirlenmiş olur ve ilgili veri paketinin tekrar gönderilmesi sağlanır. Bu sayede ilgili veri paketlerinin alıcıya ulaşıp ulaşmadığı belirlenmektedir [6].

İki kullanıcı arasında TCP ile bir bağlantı kurulmak istendiğinde, kullanıcılar arasında bir dizi mesaj değiş-tokuşu yaşanmaktadır. Bu mesaj alışverişine TCP üçlü el sıkışması denmektedir ve standart bir TCP üçlü el sıkışmasının içeriği şu şekildedir:

- A kullanıcısı, B kullanıcısına synchronize (SYN, senkronize) paketi gönderir.
- B kullanıcısı kendisine gelen istek paketini aldığını belirtmek için ACK-SYN paketi ile cevap verir.
- A kullanıcısı, B kullanıcısına ACK paketi gönderir. Bu paketin iletilmesinden sonra iki kullanıcı arasında TCP bağlantısı kurulmuş olur.



Şekil 2.3: TCP bağlantı örneği.

Veri iletimi sırasında, veriler küçük paketlere bölünür ve farklı sıralar ile ilgili alıcıya gönderilir. TCP protokolü farklı sıralar ile gelen verinin doğru bir sıralama ile alıcıya ulaşmasını sağlamaktadır.

2.1.3. User Datagram Protocol (UDP, Kullanıcı Veri Bloğu İletim Protokolü)

Kullanıcı veri bloğu iletim protokolü, OSI referans modelinin dördüncü katmanı olan taşıma katmanında kullanılmaktadır. UDP protokolü ile ses, görüntü ve video gibi verilerin gerçek zamanlı olarak hızlı bir şekilde iletilmesi sağlanmaktadır. UDP, ilgili veri paketlerinin alıcıya ulaşıp ulaşmadığını kontrol etmez. Bu nedenle TCP protokolüne göre daha hızlı bir protokol olmasına rağmen doğruluk ve güvenlik konularında oldukça zayıf bir protokoldür.

UDP bağlantısı sırasında, ilgili paketlerin alıcıya ulaşıp ulaşmadığı kontrol edilmez ve iletilmeyen bir veri paketinin alıcıya tekrar iletilmesi sağlamaz. Bu sayede veri iletim süresi en aza indirgenmiş olur. UDP, hızlı iletişim kurulması gereken yerlerde ve ilgili paketlerin teslim edileceğine dair bir garanti gerektirmeyen uygulamalar için tercih edilen bir protokoldür [7].

2.1.4. Real-time Transport Protocol (RTP, Gerçek Zamanlı İletim Protokolü)

Gerçek zamanlı iletim protokolü, gecikmeye karşı hassas olan ses, video ve telekonferans gibi gerçek zamanlı çoklu ortam verilerinin uçtan uca iletilmesini sağlamak için geliştirilmiş bir standarttır. RTP, çoklu ortam verilerinin taşınmasını genellikle UDP protokolü üzerinden gerçekleştirmektedir. RTP protokolü, ilgili paketin alındığına dair UDP protokolüne sıra numarası ve zaman bilgisi bitlerinin eklenmesini sağlar. Eklenen sıra numarası bilgisi ile alıcıya ulaşan paketlerin numaralarına bakılarak doğru bir şekilde sıralanması sağlanır ve paket kaybı yaşanıp yaşanmadığı tespit edilir. Eklenen zaman bilgisi ile gelen veri paketlerinin senkronize olması sağlanır ve paketlerde karşılaşılabilecek gürültü gibi problemler giderilmeye çalışılır [8,9].

2.1.5. Real-time Transport Control Protocol (RTCP, Gerçek Zamanlı Denetim İletim Protokolü)

Gerçek zamanlı denetim iletim protokolü, RTP oturumundaki kullanıcılara düzenli olarak kontrol paketleri gönderilmesini sağlayarak, oturumdaki hizmet kalitesinin izlenmesi için kullanılmaktadır. Gönderilen kontrol paketleri, oturumdaki kullanıcılara ait bilgilerin yanı sıra oturuma katılan kullanıcı sayısı ve oturumdan ayrılan kullanıcı sayısı gibi bilgileri de içermektedir.

RTP oturumu sırasında tüm kullanıcılar birbirlerine RTCP paketleri göndererek oturum hizmet kalitesinin denetlenmesini sağlarlar. Gönderilen RTCP paketleri ile oturumdaki kullanıcıların

sağlayabileceği hizmet kalitesi ve kullanıcılara sunulabilecek hizmet kalitesi belirlenir. Oturum hizmet kalitesinin belirlenebilmesi için gelen paket sayısı, giden paket sayısı, kayıp paket sayısı, kayıp paket oranı, paket gecikme süresi gibi veri kalitesini belirleyen parametreler ile istatistik raporları hazırlanır ve RTP protokolüne hizmet kalitesi için geri bildirim olarak iletilir [8,9].

2.1.6. H.323 Protokolü

H.323 protokolü, gerçek zamanlı ses, görüntü ve video gibi çoklu ortam verilerinin iletilmesi için International Telecommunications Union (ITU, Uluslararası Telekomünikasyon Birliği) tarafından geliştirilmiş bir standarttır. Yerel ağlar üzerinde çoklu ortam uygulamaları için geliştirilmiş olan H.323 protokolü, günümüzde yaygın olarak IP tabanlı uygulamalarda yalnızca ses iletimi için kullanılmaktadır.

VoIP teknolojisinde sinyalleşme protokolü olarak tercih edilen H.323 standardı ses kodlama, video kodlama, çoklama ve yayın senkronizasyonu gibi birçok yeteneğe sahiptir. Ancak bu yeteneklerinin birçoğu kullanılmamaktadır.

H.323 tabanlı bir VoIP iletişiminde hem TCP protokolü hem de UDP protokolü kullanılmaktadır. Veri iletişimi sırasında sinyallerin düzenli olarak iletilmesi gerekir. TCP protokolü ile ilgili sinyallerin ulaşıp ulaşmadığı kontrol edilir ve ulaşmayan sinyal var ise tekrar gönderilmesi sağlanarak veri kaybının önüne geçilir. UDP protokolü ise paket kaybının önemli olmadığı yalnızca ses paketlerinin hızlı iletilmesi gerektiği durumlarda kullanılır [10].

VoIP haberleşmesinde yaygın olarak kullanılan sinyalleşme protokolleri arasında gösterilen H.323 standardı, son yıllarda popülerliğini yitirmeye başlamıştır. H.323 protokolü için iyileştirmelerin ve geliştirmelerin yapılmaması popülerliğini yitirme nedenlerinden biri olarak gösterilebilir [11].

2.1.7. Media Gateway Control Protocol (MGCP, Ortam Geçit Kontrol Protokolü)

Ortam geçit kontrol protokolü, analog ses ve paket dönüşümünü sağlayan ağ cihazları (ortam geçitleri) arasında bağlantı kurulmasını sağlayarak, farklı ağlar arasında ses verisinin iletilmesi için geliştirilmiş bir standarttır. SGCP (Bell Core) ve IPDC (Level 3 Communication) protokollerinin birleşimi olan MGCP, master/slave mimarisinde çalışan metin tabanlı bir protokoldür.

VoIP teknolojisinde sinyalleşme ve çağrı protokolü olarak kullanılan MGCP standardı, herhangi bir oturum kurulmadan önce ağ cihazları arasında ilgili portların tahsis edilmesi ve uygun codec seçimi için Session Description Protocol (SDP, Oturum Tanımlama Protokolü) 'nü kullanmaktadır [12].

2.1.8. Session Initiation Protocol (SIP, Oturum Başlatma Protokolü)

Oturum başlatma protokolü, internet ağı üzerinden çoklu ortam görüşmelerinin yapılabilmesi için Internet Engineering Task Force (IETF) tarafından geliştirilmiş bir standarttır. SIP, iki ya da daha fazla kullanıcı arasında çoklu ortam oturumlarının kurulmasını, yönetilmesini ve sonlandırılmasını sağlayan bir sinyalleşme ve kontrol protokolüdür [13,14].

VoIP haberleşmesinde yaygın olarak kullanılan sinyalleşme protokolleri arasında gösterilen SIP protokolü, son yıllarda popülerliğini arttırmaya başlamıştır. SIP protokolünün diğer sinyalleşme protokollerine göre daha basit bir yapıya sahip olması ve daha kolay yönetilebilir olması popülerliğinin artmasını sağlamaktadır.

2.2.SIP MİMARİSİ

SIP, IP ağı üzerinden çoklu ortam görüşmelerinin yapılabilmesini sağlamak amacıyla IETF tarafından geliştirilmiş bir sinyalleşme ve kontrol protokolüdür. İki ya da daha fazla kullanıcı arasında çoklu ortam oturumlarının kurulmasını, yönetilmesini ve sonlandırılmasını sağlayan SIP protokolü, RFC 2543 ile tanımlanmış ve RFC 3261 ile geliştirilmiştir [13].

SIP oturumunun başlatılabilmesi için gerekli olan parametrelerin (kullanıcı adı, lokasyon bilgisi, vb.) tanımlanması ve gerekli ara işlemlerin yapılması ile kullanıcılar arasında başarılı bir oturum kurulması sağlanmaktadır. Kurulan SIP oturumlarında ses, görüntü ve video iletiminin dışında anlık mesajlaşma, sesli ve görüntülü telekonferans yapılabilme imkânı da sunulmaktadır.

Hyper Text Transfer Protocol (HTTP, Hiper Metin Aktarım Protokolü) ve Simple Mail Transfer Protocol (SMTP, Basit Mail Aktarım Protokolü) standartları temel alınarak geliştirilen SIP, metin tabanlı bir yapıya sahiptir. Metin tabanlı oluşundan dolayı esnek ve basit bir yapısı olan SIP protokolüne, zamanla yeni özellikler kazandırılabilir ve iyileştirmeler sağlanabilir.

SIP tabanlı bir VoIP iletişiminde hem UDP protokolü hem de TCP protokolü desteklenmektedir. İlgili paketlerin iletimi sırasında 5060 portunu kullanan UDP, önceliğin gerçek zamanlı paket iletimi olduğu durumlarda tercih edilmektedir. Herhangi bir üçlü el sıkışma mekanizmasına sahip olmadığı için paket kaybı yaşanabilir ancak paketler hızlı bir şekilde ve anlık olarak gönderilir. TCP ise önceliğin güvenli paket iletimi olduğu durumlarda tercih edilmektedir. Üçlü el sıkışma mekanizmasına sahip olan TCP ile paket kaybının önüne geçilir ancak paket iletiminde gecikmeler yaşanmaktadır [13,14].

VoIP haberleşmesinde sinyalleşme için çeşitli protokoller kullanılmaktadır. Ancak birçok protokol ile entegre olabilmesi ve yönetimin basit olması ile SIP, diğer sinyalleşme protokollerine göre daha yaygın bir kullanıma sahiptir ve popülerliği her geçen gün artmaktadır.

2.2.1. SIP Temel Fonksiyonları

SIP protokolü, kullanıcılar arasında başarılı bir oturumun kurulabilmesi ve yönetilebilmesi için bazı temel fonksiyonları desteklemektedir. SIP, bu temel fonksiyonların kullanabilmesi için farklı protokoller ile entegre olarak çalışmaktadır [15,16].

Kullanıcı Konumu: Oturumdaki kullanıcılar farklı cihazlardan bağlantı kurabildikleri gibi yerel ağda farklı IP adresleri üzerinden de bağlantı kurabilirler. Bu nedenle kullanıcıların güncel konumlarının belirlenmesi oldukça önemli bir konudur. Kullanılan cihaza ait güncel IP adres bilgisi elde edilerek, kullanıcının güncel konum bilgisine erişilmektedir. SIP oturumunun kurulabilmesi için kullanıcı ve sunucu arasında IP adresi ve kullanıcı adı tanımlanarak, kullanıcının ilgili sunucuya kayıt olması sağlanır. Bu sayede kullanıcı, sunucu tarafından tanınır ve sunucuya kayıtlı diğer kullanıcılar ile bağlantı kurabilir.

Kullanıcı Erişilebilirliği: Oturumdaki kullanıcıların erişilebilirlik durumlarının kontrol edilmesini sağlayan bir fonksiyondur. Kullanıcı, kendisini çevrimiçi, meşgul, dışarda ya da hemen dönecek gibi durumlarda gösterebilir. Kullanıcı erişilebilir durumda ise diğer kullanıcılar tarafından sesli ya da görüntülü görüşmeye davet edilebilir.

Kullanıcı Yetenekleri: SIP protokolü farklı platformlar ve farklı uygulamalar tarafından tercih edilmektedir. Bu nedenle oturum sırasında kullanıcıların desteklediği özellikler birbirinden farklılık gösterebilir. Kullanıcı yetenekleri, kullanılan uygulamanın özelliklerine ve oturum anındaki görüşme parametrelerine bağlı olarak hesaplanmaktadır. Örneğin, SIP oturumu

sırasında bazı kullanıcıların sesli ve görüntülü görüşme desteği bulunurken, diğer kullanıcıların yalnızca sesli görüşme desteği bulunabilir. Kullanıcı yeteneklerinin hesaplanması ile kullanıcılar arasında oturumda kullanılacak özelliklerin belirlenmesi, karşılıklı olarak aynı özelliklerin ve parametrelerin kullanılması sağlanmaktadır.

Oturum Başlatma: Oturumdaki kullanıcıların bağlantı kurmalarını sağlayan fonksiyondur. SIP oturumuna katılan kullanıcıların, bağlantı kurabilmelerini sağlayan bazı programlara sahip olmaları ve çağrı kurulumuna dair temel adımları uygulamaları gerekmektedir. SIP oturumunun kurulması sırasında kullanıcıya sesli ya da görüntülü görüşme davetinde bulunulur. Aranılan kullanıcı, bu davete karşılık kabul ya da ret mesajları gönderebilir. Kullanıcının gelen görüşme isteğine karşı kabul mesajı göndermesi durumunda oturum parametreleri üzerinde anlaşılır ve bağlantı kurulur. Böylece iki kullanıcı arasında iletişim kurabilmelerini sağlayacak olan SIP oturumu başlatılmış olur.

Oturum Yönetimi: Oturum esnasında oturum özelliklerinin değiştirilmesini sağlayan fonksiyondur. Oturum sırasında, kullanıcılar arasında iletilen veri tipleri ve kurulmuş olan bağlantının özellikleri değiştirilebilir. Örneğin, sesli görüşme yapılan bir oturum, görüntülü görüşme yapılan bir oturuma dönüştürülebilir. Yapılan görüşmeye yeni bir kullanıcı eklenebilir ya da mevcut kullanıcılar görüşmeden çıkartılabilir, kullanıcılar beklemeye alınabilir ve oturum sonlandırılabilir.

2.2.2. SIP Bileşenleri

İstemci-sunucu mimarisi mantığına sahip olan SIP protokolü, ağ üzerinde oturum kurulabilmesi için çeşitli bileşenlere ve protokollere ihtiyaç duymaktadır. Oturum sırasında kullanıcıların birbirleriyle iletişim kurabilmeleri için bileşenler kullanılırken, bileşenler arasında veri iletiminin sağlanabilmesi için protokoller kullanılmaktadır.

Kullanıcı birimi ve ağ sunucusu, SIP iletişiminde yer alan iki temel bileşendir. Bu bileşenlerden ağ sunucusu, yeteneklerine göre farklılık gösterebilmektedir [15,16].

User Agent (UA, Kullanıcı Birimi)

Kullanıcı birimi, SIP mesajları oluşturmak ve almak amacıyla kullanılan, çağrıyı başlatan ya da hedefteki aranan birim olarak tanımlanır. Kullanıcı birimi yeteneklerine göre istemci ya da sunucu olarak sınıflandırılabilir. Bir oturumun başlatılabilmesi için istekte bulunduğu durumda

istemci (UAC, User Agent Client) rolünde iken, gelen isteği cevapladığı durumda sunucu (UAS, User Agent Server) rolündedir. Kullanıcı birimi istemcileri, genellikle bilgisayar ya da telefon gibi kişisel cihazlara yüklü yazılımlar ve IP telefonlardır. Kullanıcı birimi sunucuları ise çağrıların cevaplanmasını sağlayan birimlerdir.

Bir oturum sırasında kullanıcı birimi, istemci ve sunucu rollerini dönüşümlü olarak üstlenerek uçtan uca bir veri iletişimi sağlamaktadır. İstemci rolü ile bir istek mesajı gönderilmesi sağlanırken, sunucu rolü ile gelen isteğe cevap verilmesi sağlanacaktır ve bu işlemler oturum sonlandırılana kadar devam edecektir [3,15].

SIP Server (SIP Sunucusu)

SIP sunucusu, kullanıcı isimlerinin çözümlenmesi ile IP adreslerine erişilmesini ve verinin kullanıcılar arasında iletilmesini sağlayan bileşendir. Bu bileşen ile mesajların kullanıcılar arasında doğru bir şekilde iletilmesi sağlanır. Kullanıcılar, ağ üzerindeki güncel konumlarına karşılık gelen IP adresleri ve kullanıcı isimleri ile SIP sunucusuna kayıt olurlar. Bu kayıt işlemi, kullanıcıların erişilebilir olduğunu ve diğer kullanıcılar tarafından oturuma davet edilebileceğini belirtmektedir. Sonrasında SIP sunucusu, oturuma davet edilen kullanıcının erişilebilirliğinin kontrol edilmesini sağlar. Kullanıcı erişilebilir durumda ise, SIP sunucusu tarafından kullanıcı adı ve IP adresi ile konumu belirlenir. Eğer oturuma davet edilen kullanıcı farklı bir konumda bulunuyorsa ya da farklı bir SIP sunucusuna kayıtlı ise, oturum isteği ilgili SIP sunucusuna yönlendirilir.

SIP oturumunda kullanıcı mesajları iletilirken, SIP sunucusu yeteneklerine göre kayıt sunucusu, vekil sunucusu ya da yönlendirme sunucusu gibi farklı roller üstlenmektedir [15,16,17].

Kayıt Sunucusu: Kayıt sunucusu, ağa kayıt olan kullanıcılara ait konum bilgilerinin saklanmasını sağlar. Kullanıcılar, IP adresleri ve kullanıcı isimleri ile sunucu tarafından ağa kaydedilir ve kayıt bilgileri veri tabanında saklanır. Bu sayede, ağa kayıt olan kullanıcıların konum bilgileri güncel bir şekilde tutulur. Sunucuya kayıtlı bir kullanıcı oturum başlatmak istediğinde, sunucu tarafından konum doğrulaması yapılır ve hedef kullanıcıya ulaşılması sağlanır.

Vekil Sunucusu: Vekil sunucu, bir kullanıcı tarafından iletilen mesajların, kullanıcı adına hedef kullanıcıya ya da hedef kullanıcının kayıtlı olduğu bir başka SIP sunucusuna

gönderilmesini sağlar. Kullanıcı adına hareket edebilme imkânı sağlayan vekil sunucunun tercih edildiği durumlarda kimlik doğrulama, güvenlik ve yetkilendirme gibi fonksiyonlar kullanılabilmektedir.

Yönlendirme Sunucusu: Yönlendirme sunucusu, bir kullanıcı tarafından bağlantı kurulmak istenen hedef kullanıcıya erişilmesini sağlar. Bir kullanıcı oturum başlatma isteğinde bulunduğunda, yönlendirme sunucusu hedef kullanıcının IP adresi ile cevap döner. Yönlendirme sunucusu ile kullanıcılara, hedef kullanıcıya nasıl bağlanacaklarına dair yol gösterilmektedir. Oturum başlatma isteği, paralel olarak aynı anda birden fazla konuma iletilebilir. Örneğin, bir kullanıcının iki ofiste çalıştığı bir senaryoda, kullanıcının bulunduğu ofisten bağımsız olarak gelen isteği yanıtlama imkânı bulunur.

2.2.3. SIP Adresleri

SIP protokolünde bileşenler, e-posta adresleri ile benzer yapıya sahip SIP adresleri ile tanımlanırlar. SIP adresleri; "sip:kullanıcı_adı@alan_adı" şeklinde gösterilir. Burada, "kullanıcı_adı" alanı kullanıcıya ait bir ismi ya da telefon numarasını temsil ederken; "alan_adı" alanı bir etki alanını ya da IP adresini temsil etmektedir. SIP adreslerinin gösterim şekli için SIP URI kavramı kullanılabilir. SIP URI kavramına ilişkin örneklere aşağıda yer verilmiştir [15]:

- kubra@sencar.com
- 2122207080@treo.com
- 2122207080@192.168.1.34
- kubra@192.168.1.8

2.2.4. SIP Mesajları

Metin tabanlı bir yapıya sahip olan SIP protokolü, istemciler ve sunucular arasında bilgi aktarımını sağlamak amacıyla birtakım özel mesajlar kullanmaktadır. SIP bileşenleri arasında iletilen bu özel mesajlar, istek mesajları ve cevap mesajları olarak sınıflandırılmaktadır. Bu mesajların iletimi sırasında, bileşenler arasında kimlik bilgileri paylaşılır. SDP protokolü ile bu verilerin iletilmesi sağlanır. SDP, gerçek zamanlı oturum başlatma parametrelerini tanımlamak için kullanılan bir standarttır [18].

İstemci-sunucu mimarisi mantığına sahip olan SIP protokolünde, bileşenler arasında istek (request) mesajları ve cevap (response) mesajları gönderilir. Kullanıcıdan sunucuya gönderilen mesajlar, istek mesajları olarak adlandırılır iken; sunucudan kullanıcıya gönderilen mesajlar, cevap mesajları olarak adlandırılmaktadır [15,19].

SIP İstek Mesajları

İstek mesajları, SIP oturumuna ilişkin taleplerde bulunmak amacıyla kullanıcılardan sunuculara gönderilen mesajlardır. SIP oturumunda kullanılan istek mesajları aşağıdaki gibi listelenmektedir:

Register: Kullanıcıların, ağ üzerindeki güncel konumlarına karşılık gelen IP adresleri ve kullanıcı isimleri ile SIP kayıt sunucusuna kayıt olmak için gönderdikleri istek mesajlarıdır. Sunucunun gelen isteği kabul etmesi durumunda, kullanıcı ilk kez erişilebilir olarak nitelendirilir ve diğer kullanıcılar tarafından oturuma davet edilebilir.

Invite: Kullanıcının, başka bir kullanıcıya SIP oturumu başlatmak için gönderdiği istek mesajıdır. Bu mesajın iletimi sırasında, bileşenler arasında kimlik bilgileri ve oturum parametreleri SDP protokolü aracılığı ile paylaşılır. Kullanıcının gelen isteği kabul etmesi durumunda, iki kullanıcı arasında SIP oturumu kurulur.

Ack: Kullanıcının, oturum başlatma isteğini kabul etmek için gönderdiği istek mesajıdır.

Options: Oturumdaki sunucuların ve diğer kullanıcıların yeteneklerini ve desteklediği özellikleri sorgulamak için gönderilen istek mesajıdır. Oturum sırasında kullanıcıların ve sunucuların desteklediği özellikler farklılık gösterebilir.

Subscribe: Oturumdaki kullanıcıların erişilebilirlik durumlarını kontrol etmek için gönderilen istek mesajlarıdır. Bu mesaj ile kullanıcıların çevrimiçi, meşgul, dışarda gibi durumları hakkında bilgi edinilir.

Cancel: Oturum kurulumu sırasında, kullanıcının çağrı başlatma isteğini iptal etmek için gönderdiği istek mesajıdır. Cancel mesajı, oturum başlatma isteğine herhangi bir yanıt gelmeden önce gönderilir. Oturum başlatma isteği kabul edilmiş ve kullanıcılar arasında oturum kurulmuş ise Cancel mesajı kullanılamaz.

Bye: Kullanıcının, oturumu sonlandırmak için gönderdiği istek mesajıdır. Oturumu sonlandırmak isteyen kullanıcı BYE mesajını göndererek, isteğini karşı tarafa iletir. Çok kullanıcılı oturumlarda, yalnızca BYE isteği gönderen kullanıcının oturumu sonlandırılır, diğer kullanıcılar arasında oturum devam eder.

SIP Cevap Mesajları

Cevap mesajları, istek mesajlarına karşılık olarak sunucuların kullanıcılara gönderdiği mesajlardır. SIP metin tabanlı bir protokol olduğu için cevap mesajları, gönderilecek yanıtlar için durum kodları ve kısa açıklamalar içerir. SIP oturumunda; gönderilen istek mesajlarına karşılık olarak kullanılabilecek cevap mesajları, altı kategori altında incelenmektedir [15,19,20].

Bilgilendirme Mesajları (1xx): İstek mesajının alındığını ve işlem aşamasında olduğunu belirtmek için gönderilen cevap mesajlarıdır.

Başarı Mesajları (2xx): İstek mesajının alındığını ve onaylandığını belirtmek için gönderilen cevap mesajlarıdır.

Yönlendirme Mesajları (3xx): İstek mesajı için işlemlerin tamamlanmadığını, aktarma ya da yeniden yönlendirme gibi ek işlemlerin yapılması gerektiğini belirtmek için gönderilen cevap mesajlarıdır.

Kullanıcı Hataları (4xx): İstek mesajında kullanıcı kaynaklı hataya rastlanıldığını ve sunucunun işlemi gerçekleştiremediğini belirtmek için gönderilen cevap mesajlarıdır. Örneğin, mesajın yanlış sözdizimine sahip olması kullanıcı kaynaklı bir hatadır.

Sunucu Hataları (5xx): İstek mesajının alındığını ancak sunucu kaynaklı bir hataya rastlanıldığını ve sunucunun gelen isteği yerine getiremeyeceğini belirtmek için gönderilen cevap mesajlarıdır.

Genel Hatalar (6xx): Genel hataları belirtmek için gönderilen cevap mesajlarıdır.

Yaygın olarak kullanılan SIP cevap mesajları aşağıdaki gibidir:

Tablo 2.2: SIP cevap mesajları.

100	Trying (Deniyor)
180	Ringing (Çalıyor)
181	Call is Being Forwarded (Arama Yönlendiriliyor)
182	Queued (Sıraya Alındı)
183	Session Progress (Oturum Devam Ediyor)
200	OK (Tamam)
202	Accepted (Kabul Edildi)
300	Multiple Choices (Çoklu Seçenekler)
301	Moved Permanently (Kalıcı Olarak Yeri Değişti)
302	Moved Temporarily (Geçici Olarak Yeri Değişti)
400	Bad Request (Geçersiz İstek)
401	Unauthorized (Yetkisiz Kullanım)
402	Payment Required (Ödeme Gerekiyor)
403	Forbidden (Yasak)
404	Not Found (Bulunamadı)
405	Method Not Allowed (İzin Verilmeyen Yöntem)
406	Not Acceptable (Kabul Edilemez)

408	Request Timeout (İstek Zaman Aşımı)
415	Unsupported Media Type (Desteklenmeyen Medya Tipi)
500	Server Internal Error (Dahili Sunucu Hatası)
502	Not Implemented (Geçerli Değil)
503	Service Unavailable (Hizmet Erişilemez)
600	Busy Everywhere (Her Yer Meşgul)
603	Decline (Reddedilme)
606	Not Acceptable (Kabul Edilemez)

2.2.5. SIP Mesaj Bölümleri

SIP protokolünde, istemciler ve sunucular arasındaki iletişimi sağlamak amacıyla SIP mesajları kullanılmaktadır. SIP mesajları; başlangıç satırı, başlık ve gövde olmak üzere üç temel bölümden oluşmaktadır [16].

Başlangıç Satırı

Tüm SIP mesajları bir başlangıç satırı ile başlamaktadır. Başlangıç satırı, mesaj türüne göre istek ya da durum satırı olabilir. İstek satırı ile yöntem türü belirtilir iken; durum satırı ile cevap kodu belirtilir.

İstek satırı, bağlantı kurulmak istenen kullanıcıyı ya da alınmak istenen hizmeti belirten SIP URI adresini ve protokol versiyonunu içermektedir. Durum satırı ise nümerik cevap kodunu, bu kod ile ilişkilendirilmiş açıklamayı ve protokol versiyonunu içermektedir.

Başlık

Metin tabanlı bir mimariye sahip olan SIP; mesaj başlık yapısı, söz dizimi ve semantik açıdan HTTP ile benzerlik göstermektedir. SIP başlıkları, mesajın anlamını değiştirmek ve mesaj

özelliklerini taşımak amacıyla kullanılmaktadır. SIP başlık yapısı aşağıdaki şekilde gösterilebilir:

<isim>:<değer>

Gövde

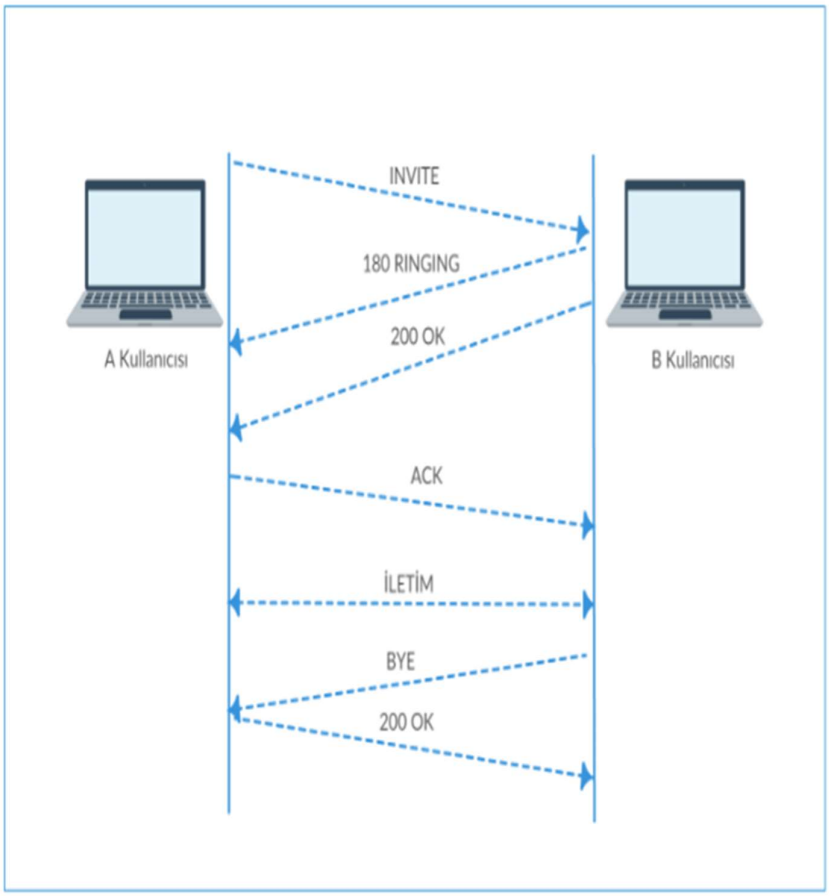
SIP mesaj gövdesi, kurulacak olan oturumu tanımlamak ve oturuma ilişkin verileri ikili düzende ya da metin tabanlı olarak iletmek için kullanılır. İstek mesajlarında ve cevap mesajlarında kullanılmaktadır.

Gövde kısmında, oturum tanımlaması için yaygın olarak SDP protokolü kullanılır. Bileşenler arasında mesaj iletimi sırasında SDP bilgisi de paylaşılır. Bu sayede, oturum parametreleri üzerinde uzlaşma sağlanmış olur.

2.2.6. SIP Çağrı Akışı

SIP oturumu sırasında bileşenler arasındaki iletişimi ve etkileşimi inceleyebilmek için SIP çağrı akışı ele alınmıştır. Bir kullanıcı, diğer kullanıcılar ile bağlantı kurabilmek ve veri iletişimini başlatabilmek için çeşitli sunuculara mesajlar gönderir. Diğer kullanıcılar ile arasında bir oturum başlatılana kadar, istemci-sunucu mimarisinden bahsedilmektedir. Oturum başlatma isteğinde bulunan kullanıcı, sunuculara bağlantı isteğinde bulunur ve bulunduğu istek için cevap verilmesini bekler. Kullanıcılar arasında bağlantı kurulduktan sonra noktadan noktaya mimarisi devreye girmektedir [14,15].

Şekil 2.4'de iki kullanıcı arasında kurulan SIP oturumuna dair basit bir örnek verilmiştir. A kullanıcısı, B kullanıcısı ile çağrı başlatabilmek için "INVITE" mesajı gönderir. B kullanıcısı, istek mesajının alındığını ve onaylandığını belirtmek için sırasıyla 180 RINGING ve 200 OK cevap mesajlarını gönderir. A kullanıcısı, "ACK" mesajı ile cevap mesajının alındığını belirtir. Bu noktadan sonra iki kullanıcı arasında oturum kurulur ve gerçek zamanlı veri iletişimi başlar. B kullanıcısı, kurulan oturumu sonlandırmak için "BYE" mesajı gönderir. Bu mesaja karşılık A kullanıcısı, isteğin onaylandığını belirtmek için 200 OK mesajını gönderir ve iki kullanıcı arasındaki oturum sonlandırılmış olur.

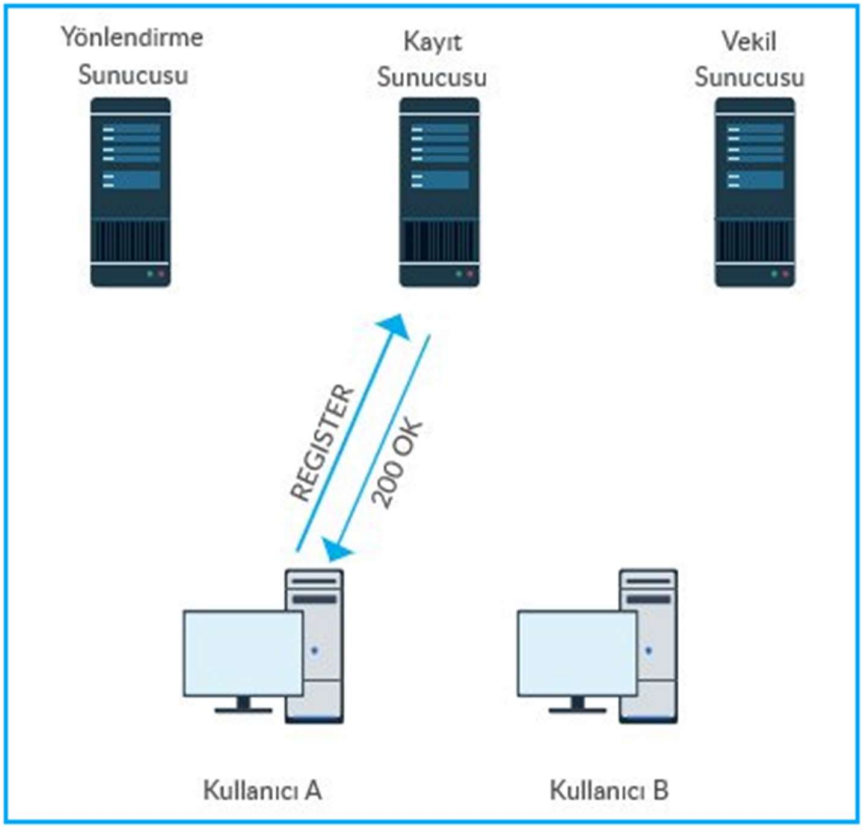


Şekil 2.4: Basit bir SIP oturum senaryosu.

Kullanıcılar, diğer kullanıcılar ile oturum başlatabilmek için farklı sunuculara çeşitli mesajlar gönderirler. Bu sunucuların aracılığı ile çeşitli çağrı kurulum senaryoları gerçekleştirilmektedir.

SIP Kayıt İşlemi

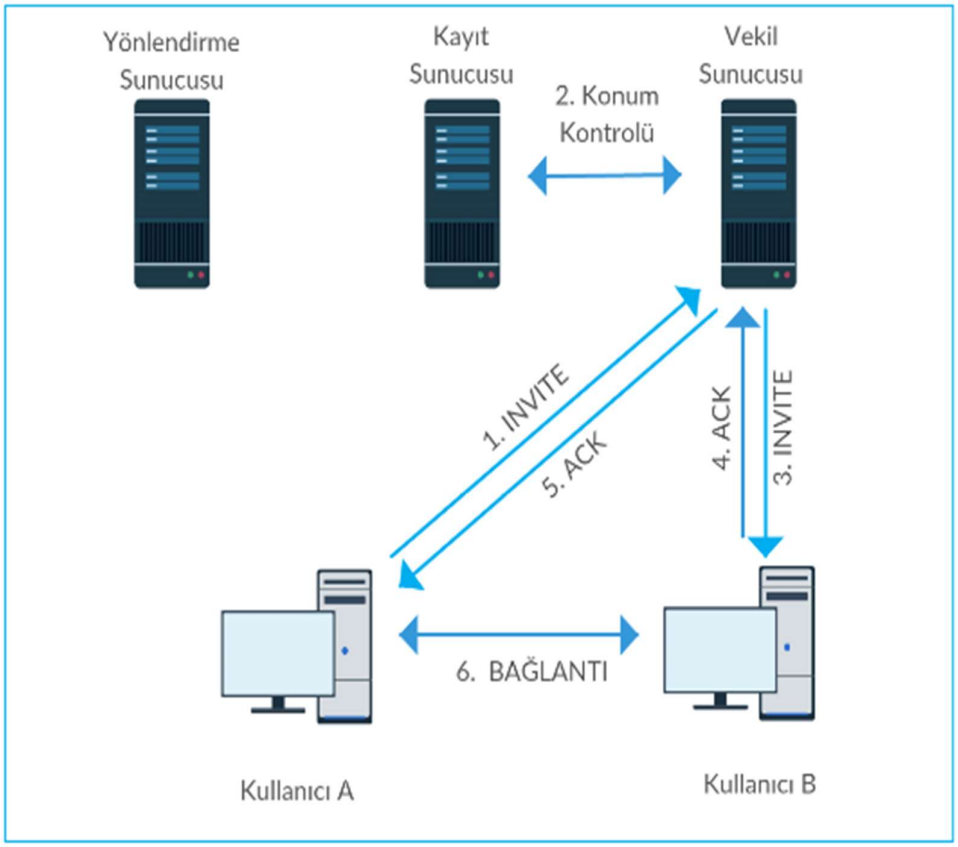
Bir kullanıcının, diğer kullanıcılarla bağlantı kurabilmesi için öncelikle, bir kayıt sunucusuna bağlanması gerekir. Kullanıcı, kayıt sunucusuna "REGISTER" mesajı ile istekte bulunur. Sunucunun bu isteği kabul etmesi ile, kullanıcının IP adresi ve SIP adresi konum servisine kaydedilir ve sunucu, kullanıcıya isteğinin onaylandığına dair 200 OK mesajı gönderir. Kayıt sunucusu üzerindeki konum servisleri, kullanıcı adı aracılığı ile kullanıcının IP adresine ve SIP adresine ulaşılmasını sağlar.



Şekil 2.5: SIP sunucusuna kayıt işlemi [3,20].

Vekil Sunucu Aracılığı ile Çağrı Kurulumu

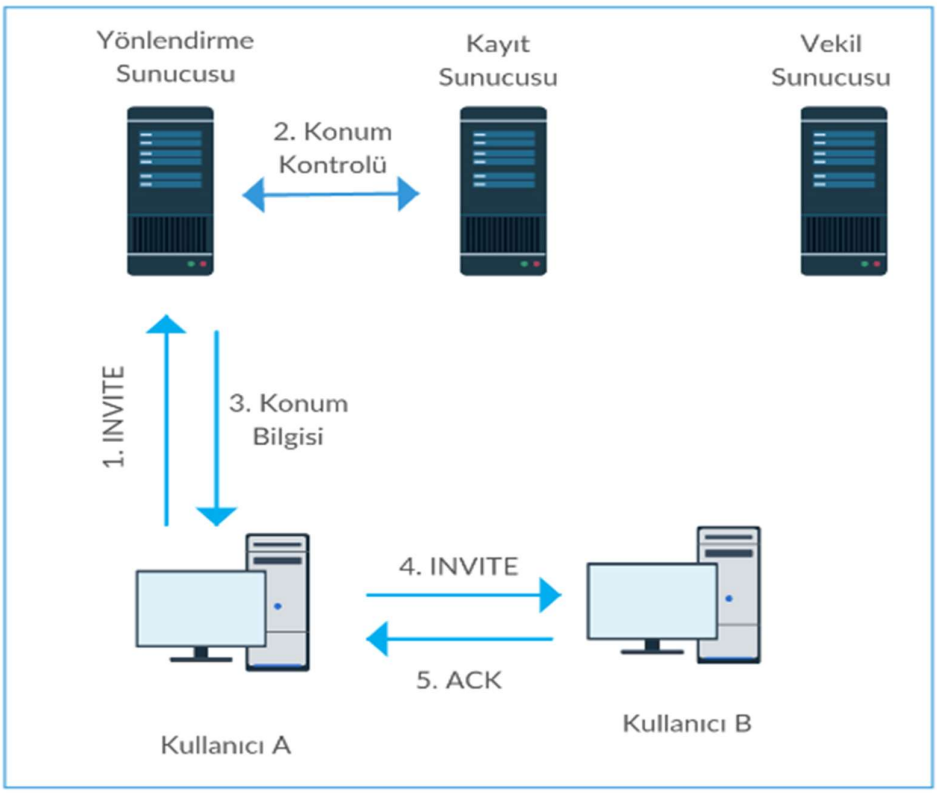
Kullanıcının, vekil sunucu aracılığı ile istekte bulunması ve cevap vermesi, vekil sunucu üzerinden yönlendirmeli bir bağlantı kurduğunu gösterir. Şekil 2.6'da, iki kullanıcı arasında vekil sunucu aracılığı ile kurulan SIP oturumuna dair basit bir örnek verilmiştir. Kullanıcı A, Kullanıcı B ile oturum kurmak istediğinde, vekil sunucu üzerinden "INVITE" mesajı gönderir. Oturum kurulmak istenen kullanıcının güncel IP adresi, kayıt sunucusu üzerinde yer alan konum servisinden kontrol edilir. Güncel konum bilgisi elde edilen Kullanıcı B'ye, vekil sunucu tarafından oturum başlatma isteği iletilir. Kullanıcı B'nin cevabı, vekil sunucu üzerinden Kullanıcı A'ya iletilir. Bu noktaya kadar kullanıcılar ve vekil sunucu arasındaki sinyalleşme, SDP üzerinden gerçekleşmiştir. Vekil sunucu, her iki kullanıcıya da onay mesajı gönderir ve kullanıcılar arasında oturumun kurulmasını sağlar. Oturum kurulduktan sonra, kullanıcılar arasında gerçek zamanlı veri iletişimi için RTP kullanılır.



Şekil 2.6: Vekil sunucu aracılığı ile çağrı kurulumu [3,20].

Yönlendirme Sunucusu Aracılığı ile Çağrı Kurulumu:

Kullanıcının, yönlendirme sunucusu aracılığı ile istekte bulunması ve cevap vermesi, yönlendirme sunucusu üzerinden yönlendirmeli bir bağlantı kurduğunu gösterir. Şekil 2.7'de, iki kullanıcı arasında yönlendirme sunucusu aracılığı ile kurulan SIP oturumuna dair basit bir örnek verilmiştir. Kullanıcı A, Kullanıcı B ile oturum kurmak istediğinde, yönlendirme sunucusu üzerinden "INVITE" mesajı gönderir. Oturum kurulmak istenen kullanıcının güncel IP adresi, kayıt sunucusu üzerinde yer alan konum servisinden kontrol edilir. Yönlendirme sunucusu, güncel konum bilgisini Kullanıcı A'ya iletir. Bu sayede, Kullanıcı A'nın bağlantı kurabilmesi için gerekli bilgiye sahip olması sağlanır. Kullanıcı A, Kullanıcı B'ye oturum başlatma isteğini gönderir. Gelen oturum başlatma isteğine karşılık olarak Kullanıcı B, cevap mesajı gönderir. Bu noktaya kadar sinyalleşme, SDP üzerinden gerçekleştirilmiştir. İki kullanıcı arasında oturum kurulduktan sonra, gerçek zamanlı veri iletişimi için RTP kullanılır.



Şekil 2.7: Yönlendirme sunucusu ile çağrı kurulumu [3,20].

2.3.GÜVENLİK TEHDİTLERİ VE SALDIRILAR

Yeni nesil telekomünikasyon sektöründe, VoIP teknolojisi gün geçtikçe daha popüler bir hale gelmiştir ve hem bireysel kullanıcılar hem de kurumsal kullanıcılar arasında yaygın olarak kullanılmaya başlanmıştır. Popüler olan ve yaygın olarak kullanılan diğer teknolojiler gibi VoIP teknolojisi de saldırganların dikkatini çekmeye başlamıştır ve günümüzde özellikle bilgi güvenliği saldırılarının hedefi haline gelmeye başlamıştır.

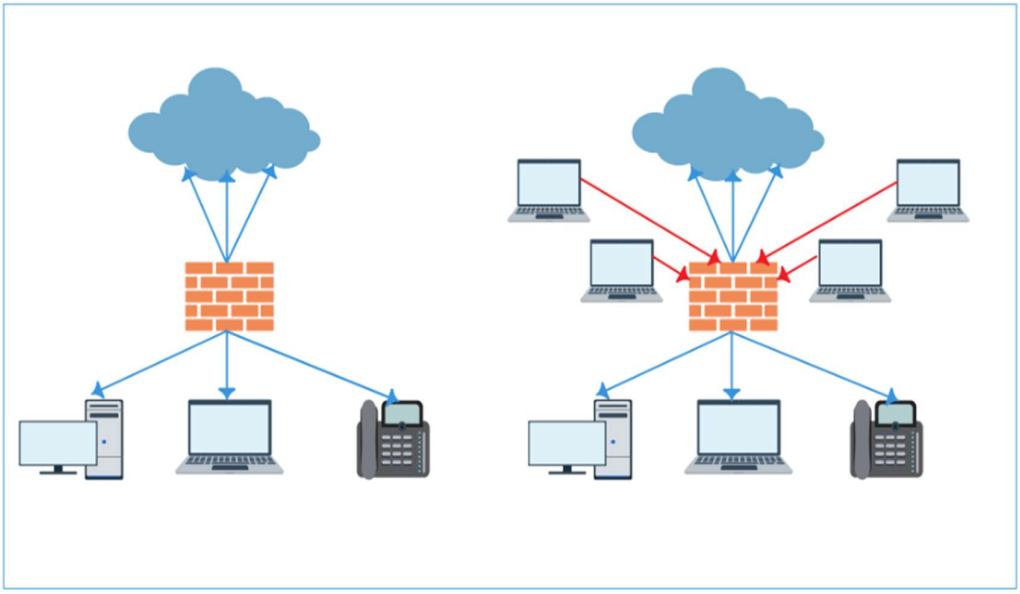
VoIP teknolojisinde güvenli protokoller, yüksek kaliteli güvenlik araçları ve yetenekli güvenlik uzmanları kullanılması durumunda bile, her geçen gün yeni güvenlik sorunları ile karşılaşılmakta ve saldırıları önlemek oldukça zor bir hale gelmeye başlamaktadır. VoIP teknolojisi, IP ağı üzerinden hizmet veren bir servistir ve IP ağı üzerinden hizmet veren diğer servisler gibi çeşitli saldırılardan etkilenmektedir. Ek olarak, yazılım ve servis konfigürasyonlarının hem üretici firmalar tarafından hem de son kullanıcılar tarafından gerçekleştirilmesi de VoIP mimarisinin çeşitli saldırılardan etkilenmesine neden olmaktadır.

Bu saldırılar, VoIP sistemlerinin gizlilik, güvenilirlik ve erişilebilirlik gibi temel özelliklerini hedef almaktadır. VoIP sistemlerini hedef alan bu saldırıların etkileri farklı boyutlarda olabilmektedir [1,2,21].

2.3.1. Denial of Service (DoS, Hizmet Reddi) Saldırıları

Hizmet reddi saldırıları, VoIP mimarisinde gerçekleştirilmesi en kolay ancak engellenmesi en zor saldırı türlerinden biridir. DoS saldırılarında, IP temelli ağlar hedef alınmakta ve sistemin geçici bir süre ya da tamamen kullanılamaz bir hale getirilmesi amaçlanmaktadır. Bu saldırılar, tek bir kaynak üzerinden gerçekleştirilebileceği gibi, birden fazla kaynak üzerinden de gerçekleştirilebilmektedir. Birden fazla kaynak üzerinden hedef olarak belirlenen ağa çok sayıda veri paketi gönderilerek gerçekleştirilen saldırılar Distributed Denial of Service (DDoS, Dağıtılmış Hizmet Reddi) olarak adlandırılmaktadır [1,2,21].

Şekil 2.8'de, DoS saldırısının hedefi haline gelmiş bir sistem görülmektedir. Şeklin sol tarafında bileşenler arasındaki trafiğin normal akşında olduğu görülür iken, şeklin sağ tarafında ise saldırganlar tarafından oluşturulan trafiğin bileşenleri etkilediği görülmektedir. Farklı dış kaynaklardan çok sayıda veri paketi alan sistemin hizmet veremez hale getirilmesi amaçlanmıştır.



Şekil 2.8: DoS saldırı senaryosu.

DoS saldırılarında, saldırgan hedef olarak belirlediği bileşene çok sayıda geçersiz ve sahte veri paketleri gönderir. Gönderilen veri paketlerinin işlenmesi sırasında işlemci, bellek ve bant genişliği gibi sistem kaynaklarının tüketilmesi, sistem bileşenlerinin zarar görmesi ve sistem kalitesinin düşmesi hedeflenir. Bunun sonucunda sistem çağrıları karşılayamaz ve kullanılamaz bir hale getirilir.

DoS/DDoS saldırıları, hedef olarak belirlenen kullanıcıya ya da sisteme çok sayıda ses paketinin gönderilmesi ile gerçekleştirilir. Gönderilen ses paketlerinin herhangi bir doğrulama mekanizmasından geçmesi ya da şifrelenmiş bir şekilde gönderilmesi bu saldırıların gerçekleştirilmesine engel olamamaktadır [1,22,23].

VoIP mimarisi gerçek zamanlı iletişimi desteklediği için veri paketlerinin iletimindeki küçük gecikmeler bile sistem üzerinde büyük etkiler yaratabilir. Saldırılardan bazıları sistemi geçici, bazıları ise tamamen hizmet veremez hale getirebilir. Yaygın olarak karşılaşılan temel DoS saldırılarını şu şekilde sıralayabiliriz:

Flooding Tabanlı DoS Saldırıları: Flooding (mesaj baskını) tabanlı DoS saldırılarında, saldırgan hedef olarak belirlediği sisteme çok sayıda paket gönderir ve işlemci, bellek ya da bant genişliği gibi sistem kaynaklarını tüketmeye çalışır. Sisteme gönderilen paket sayısı, sistemin karşılayabileceği paket sayısından daha fazladır. Saldırı sırasında, sistem kaynakları tüketildiği için yasal kullanıcılar tarafından gönderilen eş zamanlı hizmet isteklerine sistem cevap veremez. Flooding tabanlı DoS saldırıları ile sistem erişilemez hale getirilir [24].

VoIP uygulamaları, flooding tabanlı DoS saldırılarından farklı şekillerde etkilenmektedir. En sık karşılaşılan saldırıların başında UDP Flooding ve TCP-SYN Flooding yer almaktadır. UDP Flooding saldırılarında, hedef olarak belirlenen sisteme çok sayıda UDP paketi gönderilerek, sistemin diğer kullanıcılar için erişilemez hale getirilmesi amaçlanır. TCP-SYN Flooding saldırılarında ise, hedef olarak belirlenen sisteme ardışık olarak çok sayıda SYN paketleri gönderilerek, sistemin yasal kullanıcılara cevap veremeyecek hale getirilmesi amaçlanır.

Paket Tekrarlama Tabanlı Saldırılar: Paket tekrarlama tabanlı saldırılarda, gönderilen bir veri paketi saldırgan tarafından ele geçirilir. Ele geçirilen bu veri paketi sisteme sürekli olarak gönderilir. Sürekli gönderilen veri paketleri sistem üzerinde trafik oluşmasına neden olduğu gibi hedefe iletilmiş olan veri paketlerinin sıralamasını da etkiler. Bunun sonucunda ses paketlerinin iletiminde gecikme yaşanır ve hizmet kalitesi düşer.

TLS Bağlantısı Sıfırlama Tabanlı Saldırılar: TLS bağlantısı sıfırlama tabanlı saldırılarda, kullanıcı ve sunucu arasındaki sinyalleşmenin güvenli bir şekilde gerçekleşmesini sağlayan TLS bağlantısı sıfırlanır. Hedef olarak belirlenen sisteme, bir komut gönderilerek TLS bağlantısı sıfırlanır. Bu saldırı sonucunda, kullanıcı ve sunucu arasındaki güvenli sinyalleşme bozulmuş olur.

Paket Ekleme Tabanlı Saldırılar: Paket ekleme tabanlı DoS saldırılarında, saldırgan veri paketlerini ele geçirir. Ele geçirilen veri paketlerinin içerisine yeni kelimeler, boşluklar ya da gürültü eklenerek yeni veri paketleri oluşturulur. Saldırgan, hedef olarak belirlediği sisteme oluşturduğu paketlerden çok sayıda gönderir. Böylece sistemin hizmet kalitesi düşürülmüş olur. Sistemde herhangi bir yetkilendirme yapılmamış ise, RTCP paketlerine müdahale edilmesi ile paket ekleme tabanlı saldırılar gerçekleştirilir.

QoS Modifikasyon Tabanlı Saldırılar: QoS modifikasyon tabanlı saldırılarda, saldırgan veri paketleri içerisinde yer alan kontrol bitleri üzerinde değişiklikler yapar. Bu saldırı, IP paketlerindeki ToS (Terms of Service) bitlerinin değiştirilmesi ile gerçekleştirilir. Veri trafiği öne çıkarılarak, ses trafiği ikinci plana atılır. Ses trafiği ikinci plana atıldığından dolayı, ses iletişiminde gecikmeler olur ve paket kayıpları yaşanır. Böylece sistemin hizmet kalitesi düşürülmüş olur.

Çağrı Düşürme Tabanlı Saldırılar: Çağrı düşürme tabanlı DoS saldırılarında, saldırgan hedef olarak belirlediği kullanıcıya “CANCEL” ya da “BYE” paketleri göndererek çağrı kurulumunu engellemeye çalışır ya da kurulmuş olan bir çağrıyı sonlandırmaya çalışır. Saldırgan, iki farklı yöntemle çağrı düşürme tabanlı DoS saldırısını gerçekleştirebilir. İlk yöntemde hedef kullanıcı INVITE paketi alır almaz, saldırgan “CANCEL” paketi gönderir. Böylece kullanıcılar arasında oturum kurulması engellenmiş olur. İkinci yöntemde ise oturum sırasında, saldırgan hedef kullanıcıya “BYE” paketi gönderir. Böylece kullanıcılar arasında kurulmuş olan oturum sonlandırılmış olur.

Amplification Tabanlı Saldırılar: Amplification tabanlı saldırılarda, saldırgan hedef olarak belirlediği sistemin IP adresini kullanarak, ağın broadcast adresine veri paketi gönderir. Veri paketi broadcast adresine gönderildiği için, ağdaki tüm kullanıcılara iletilir. Ağ üzerindeki kullanıcıların her biri, saldırgan tarafından hedef olarak gösterilen sisteme cevap gönderir. Bu

saldırı sonucunda, hedef sistem aşırı yüklenir ve oluşan trafiği karşılayamaz. En yaygın karşılaşılan amplification saldırılarının başında, Smurf ve Fragle saldırıları gelmektedir [22,25].

2.3.2. Man In The Middle (MITM, Ortadaki Adam) Saldırısı

Ortadaki adam saldırısı, VoIP mimarisini hedef alan en önemli güvenlik tehditlerinden biridir. Saldırgan, aralarında bağlantı sağlanan kullanıcıların arasına girerek, çağrı trafiğinin kendi üzerinden akmasını sağlar. Böylece saldırgan, kullanıcılar arasındaki iletişim sırasında tüm trafiğe erişebilir, dinleyebilir, kaydedebilir ve değiştirebilir.

Ortadaki adam saldırısı, Address Resolution Protocol (ARP, Adres Çözümleme Protokolü) zehirlenmesi ile başlatılır. Saldırgan, ağ üzerindeki sunuculardaki kayıtlı olan kullanıcıların IP adresi ve MAC adresi eşleşmelerini değiştirmeye çalışır. Hedef olarak belirlediği kullanıcının ARP tablosundaki MAC adresini, kendi MAC adresi ile değiştirir. Böylece kullanıcılar arasındaki trafik, saldırganın makinesi üzerinden akmaya başlar. Bu durum oturumdaki kullanıcılar tarafından fark edilmeyebilir [1,26].

2.3.3. Ele Geçirme Saldırıları

Ele geçirme saldırılarında, saldırgan kullanıcılar arasında kurulan oturumu ele geçirir ve ele geçirdiği oturumdaki yasal kullanıcılardan birinin yerine geçer. Tüm trafik akışı, oturumdaki yasal kullanıcı yerine saldırgana ya da saldırganın belirlediği başka bir adrese yönlendirilmektedir. Bu saldırının sonucunda, yasal kullanıcıların VoIP servislerine erişmeleri engellemiş olur. Ele geçirme saldırıları; kayıt hırsızlığı ve sunucu taklidi olmak üzere iki farklı şekilde gerçekleştirilebilir [27].

Kayıt Hırsızlığı: VoIP/SIP teknolojisinde, kullanıcılar arasında bir oturum başlatılabilmesi için öncelikle, kullanıcıların SIP kayıt sunucularına kayıt olmaları gerekir. Saldırgan, kayıt işlemi sırasında kullanıcı ve sunucu arasındaki bağlantıyı izler. Yasal kullanıcıyı taklit eden saldırgan, sunucu üzerinde kayıtlı olan kullanıcı adresini, kendi adresi ile değiştirir. Bu saldırı sonucunda, tüm trafik akışı kullanıcı yerine saldırgana ya da saldırganın belirlediği adrese yönlendirilir.

Sunucu Taklidi: VoIP/SIP teknolojisinde, kullanıcılar arasında bir çağrı başlatabilmek için yönlendirme sunucusu ya da vekil sunucu kullanılabilir. Bu durumda, “INVITE” mesajları bu sunuculara gönderilir. Saldırgan, kendisini yönlendirme sunucusu ya da vekil sunucu olarak gösterebilmek için DNS sunucusunu hedef alır. Saldırgan, DNS sunucusunda bulunan

yapılandırma dosyasını, kendi oluşturduğu yapılandırma dosyası ile değiştirir. Yeni yapılandırma dosyasında, saldırganın kendi IP adresi ya da yönlendirme yapmak isteyebileceği başka bir IP adresi yer alır. Değiştirilmiş yapılandırma dosyasına göre kullanıcılar, "INVITE" mesajlarını saldırgana ait sunucuya ya da saldırganın belirlediği başka bir sunucuya göndermiş olurlar. Bu saldırı sonucunda, oturum sırasında gerçek sunucunun kullanılması engellenerek, tüm trafik akışı saldırgana ait bir sunucu üzerinden ya da saldırganın yönlendirdiği başka bir sunucu üzerinden gerçekleşir.

2.3.4. Telekulak

Telekulak saldırıları, IP ağına erişilerek; kullanıcılar arasında yapılan görüşmelerde aktarılan kişisel bilgilerin elde edilmesini hedefleyen bir saldırı türüdür. Telekulak, saldırgan tarafından kullanıcılar arasında iletilen veri paketlerine erişilmesi ve paketlerin analiz edilmesi olarak yorumlanabilir. Ağa dahil olan saldırgan, kullanıcılar arasında gerçekleştirilen çağrıyı dinleyebilir ya da kaydedebilir. Bunun sonucunda, kullanıcılara ait banka bilgileri, T.C. numarası, kullanıcı adı ve banka şifresi gibi birçok kişisel bilgi saldırgan tarafından ele geçirilebilir [1,26].

Telekulak saldırılarında, VoIP/SIP bileşenlerinin ya da protokollerinin sahip olduğu güvenlik açıklıklarından faydalanılır. Saldırgan, IP ağına erişerek; kullanıcılar arasında iletilen veri paketlerinin içeriğini bir ağ analiz programı yardımı ile inceleyebilir, dinleyebilir ve kaydedebilir. Ağ analiz programlarına internet üzerinden kolayca erişilebilmesi, VoIP sistemlerinin telekulak saldırılarına maruz kalmasına neden olmaktadır. IP ağlar üzerinden önemli kişisel verilerin iletilmemesi ve kullanıcılar arasında iletilen ses paketlerinin şifrelenerek gönderilmesi, bu saldırılara karşı verilebilecek güvenlik tavsiyeleri arasında yer almaktadır.

2.3.5. Spam over Internet Telephony (SPIT, Internet Üzerinden Spam)

Kullanıcılar tarafından istenmeyen ya da gereksiz olarak tanımlanan verilerin e-posta aracılığı ile iletilmesi spam olarak tanımlanır. Önceden kaydedilmiş, istenmeyen ya da gereksiz veriler içeren mesajların sürekli olarak kullanıcılara gönderilmesi ile gerçekleştirilen aramaların yapılması ise SPIT olarak tanımlanır. Saldırgan ticari, siyasi ya da reklam içerikli mesajlar hazırlar ve kaydeder. Sonrasında saldırgan, hedef olarak belirlediği kullanıcıya "INVITE" mesajı göndererek, oturum başlatma isteğinde bulunur. Hedef kullanıcı, oturum başlatma

isteğini kabul eder. Oturum kurulduktan sonra saldırgan, önceden kaydetmiş olduğu mesajları hedef kullanıcıya sürekli göndermeye başlar. SPIT saldırısında, hedef kullanıcı istenmeyen çağrılara ve yoğun bir trafiğe maruz bırakılarak; sistem kullanılamayacak hale getirilebilir.

VoIP mimarisi, geleneksel telefon ağlarına göre daha düşük maliyetli bir iletişim imkânı sağlamaktadır. Bu nedenle, ürün tanıtımı ya da reklam yapmak isteyen saldırganların hedefi haline gelmektedir. Saldırgan, hedef olarak belirlediği kullanıcıya gerçek zamanlı olarak siyasi, ticari ya da reklam içerikli mesajlar gönderir. Hedef kullanıcı, bu çağrının SPIT olduğunu ancak oturum kurulduktan sonra anlayabilir. Bu saldırı sonucunda kullanıcı, yoğun bir trafiğe maruz kalır ve bir süre sonra erişilemez hale gelir.

VoIP teknolojisi gerçek zamanlı iletişimi desteklediği için SPIT saldırılarının engellenmesi oldukça zordur. Buna ek olarak, SPIT saldırılarının hangi zaman aralığında ve kim tarafından gerçekleştirileceğinin belirsiz olması da bu saldırıların engellenmesini zorlaştırır. SPIT saldırılarını önleyebilmek için e-posta servislerindeki gibi kara listeler ya da beyaz listeler oluşturulabilir. Bir diğer çözüm önerisi olarak, kullanıcı doğrulaması yapılabilir. Kullanıcı doğrulamasında, arayan kişiye "Kırmızının eş anlamlısı nedir?" şeklinde basit bir soru yöneltilir. Arayan tarafın, yöneltilen soruyu cevaplama durumuna göre engelleme yapılabilir. Bu sayede SPIT saldırılarının önüne geçilebilir [28,29].

2.3.6. Ücret Dolandırıcılığı

Ülkemizde ve dünyada teknolojinin gelişmesi ile birlikte, telekomünikasyon sektöründe ücret dolandırıcılığı saldırıları karşılaşılan en önemli güvenlik tehditlerinden biri haline gelmiştir. Ücret dolandırıcılığı, telekomünikasyon dünyasında maddi kazanç elde etmek amacıyla telekom ürünlerinin ve ücretlendirme servislerinin hedef alındığı saldırı türüdür. Ücret dolandırıcılığı saldırıları; son kullanıcılar, ticari müşteriler ve servis sağlayıcılar dahil olmak üzere herkesi olumsuz olarak etkilemektedir. Bu saldırılar, servis sağlayıcıların önemli oranlarda trafik kaybı yaşamalarına ve buna bağlı olarak itibar kaybı yaşamalarına neden olmaktadır [3,29].

Ücretlendirme dolandırıcılığı saldırıları; trafik yönlendirme dolandırıcılığı ve servis sağlayıcı dolandırıcılığı olmak üzere iki farklı şekilde gerçekleştirilebilir.

Trafik Yönlendirme Dolandırıcılığı: Trafik yönlendirme dolandırıcılığında, saldırgan servis sağlayıcı trafiğinin yüksek ücretli özel hatlara yönlendirilmesini sağlar. Bu hatlara yönlendirilen trafik sonucunda, kullanıcılara normalden daha yüksek ücretler yansıtılır. Bu saldırıdan elde edilen kazanç, saldırgan ve özel hat sahiplerinin arasında paylaşılır. Trafik yönlendirme dolandırıcılığında, saldırgan hedef olarak belirlediği servis sağlayıcının sistemine erişir. Saldırgan, erişilen sisteme kayıtlı olan kullanıcıların aramalarını yüksek ücretli özel hatlara yönlendirebilir ya da kullanıcı telefonlarını taklit ederek, özel hatları arayabilir ve arama bitmeden başka bir özel hata yönlendirme yapabilir.

Servis Sağlayıcı Dolandırıcılığı: Dolandırıcılık saldırıları arasında en sık karşılaşılanı ve en kapsamlı olanı servis sağlayıcı dolandırıcılığıdır. Saldırgan, servis sağlayıcı üzerinde kayıtlı olan kullanıcıların bilgilerine erişir. Saldırgan, kendi kullanıcılarının aramalarını, ele geçirdiği kullanıcılar tarafından gerçekleştiriyormuş gibi gösterir ve hedef aldığı servis sağlayıcı üzerinden aramalar gerçekleştirir. Yapılan görüşmelerin ücreti ele geçirdiği kullanıcılar tarafından ödenirken, saldırgan kendi kullanıcısına da görüşme ücreti yansıtır. Saldırgan böylece kendi kullanıcısı üzerinden kazanç elde etmiş olur.

Başka bir servis dolandırıcılığı türünde, saldırgan servis sağlayıcı üzerindeki trafik akışını izlemektedir. Normal bir trafik akışında, kullanıcılar yanlış bir numarayı aradıklarında; “Bu numara kullanılmamaktadır.” şeklinde sesli bir mesaj ile bilgilendirilirler ve bu bilgilendirme mesajı için kullanıcılardan ek bir ücret talep edilmez. Servis sağlayıcı trafiğini izleyen saldırgan, yapılan aramayı kendisine ait otomatik cevaplama özelliği olan bir hata yönlendirir. Kullanıcı, bilgilendirme mesajını saldırganın yönlendirdiği ücretli hat üzerinden dinlediği için bir ücretlendirmeye tabi tutulur.

2.3.7. Sosyal Mühendislik

Sosyal mühendislik, saldırganın kendisini yasal bir kullanıcı gibi göstererek; hedef olarak belirlediği kullanıcıya ait kişisel bilgileri ele geçirmeye çalıştığı saldırı türüdür. Günümüzde sosyal ağ siteleri üzerinden kişisel bilgilere kolayca erişilebilmesi nedeniyle hızla artan bir ivmeye sahiptir.

Sosyal mühendislikte, saldırgan finansal kuruluşları arayarak, kendisini yasal bir kullanıcı olarak tanıtır ve yerine geçtiği kullanıcıya ait hesap bilgilerini ele geçirmeye çalışır. Başka bir sosyal mühendislik türünde, saldırgan kamu hizmeti veren kuruluşları arayarak, kendisini yine

yasal bir kullanıcı olarak tanıtır ve yerine geçtiği kullanıcıya dair kişisel bilgileri elde etmeye çalışır. Saldırgan, elde ettiği bilgiler ile kullanıcıyı arayarak, kendisini kamu hizmeti veren kuruluş olarak tanıtır ve kullanıcıyı dolandırmaya çalışır.

2.3.8. Fuzzing (Bulandırma) Saldırıları

Bulandırma, bir sistemin dayanıklılığını gözlemlemek, sistemde kullanılan protokollerin ve uygulamaların zayıf noktalarını keşfetmek için geliştirilmiş bir yazılım test tekniğidir. Bulandırma yönteminde sisteme hatalı biçimlendirilen ya da standart olmayan veri paketleri rastgele ya da sıralı olarak gönderilir. Sistemin hatalı biçimlendirilen veri paketlerine karşı davranışları incelenerek, sistemin dayanıklılığı test edilmektedir.

Bulandırma yöntemi ile sistemin zayıf noktaları ve protokollerin güvenlik zafiyetleri keşfedilmektedir. Keşfedilen bu zayıf noktalar ve güvenlik zafiyetleri, saldırganlar tarafından yeni saldırılar geliştirmek ve başlatmak için kullanılabilir. Gerçekleştirilen saldırılar sonucunda beklenmedik durumlar ile karşılaşılmaktadır. Çalışan uygulamalarda arabellek taşmaları, sonsuz döngüler ve uzun süren işlemler gözlemlenebilir. Hedef olarak belirlenen sistem ise saldırgan tarafından ele geçirilebilir ve sistem kullanılamaz hale getirilebilir.

Saldırgan, SIP ağına hatalı biçimlendirilmiş ya da standart olmayan veri paketleri gönderir ve herhangi bir cihazın ya da protokolün, bu paketlerden etkilenip etkilenmediğini kontrol eder. Eğer etkilenen herhangi bir cihaz ya da protokol var ise sistemin güvenlik açığı tespit edilmiş olur. Güvenlik açıklarını tespit ederken kullanılan hatalı biçimlendirilmiş ya da standart olmayan veri paketlerini elde etmek için basit birkaç yöntem bulunmaktadır [1,30].

Sözdizimi Hataları: Saldırgan, SIP mesajlarının sözdizimine uygun olmayan mesajlar kullanarak, sözdizimi hataları yaratabilir. Saldırgan tarafından sözdizimindeki bir parametre, hatalı bir parametre ile değiştirilir ve hatalı biçimlendirilmiş mesajlar oluşturulur. Bu hatalara, IP adres parametresine ait sözdiziminin değiştirilmesi örnek olarak verilebilir.

Contact: sip:kubra@192.168.168.168.8

Ayraç Hataları: SIP mesajlarında; alanlar, alan başlıkları ve alan değerlerinin birbirinden ayrılması için iki nokta üst üste, noktalı virgül, virgül ve boşluk karakteri gibi ayraçlar kullanılmaktadır. Standart olmayan mesajlar üretilirken; bu ayraçlar kullanılmayabilir, uygun olmayan başka bir ayraç kullanılabilir ya da ayraçlar arka arkaya kullanılabilir. From

başlığından sonra iki kere ":" kullanılması, ayraç hatalarına örnek olarak verilebilir. SIP alan başlığı ile alan değeri arasında bir kere kullanılması gereken ayracın iki kere üst üste kullanılması ile hatalı biçimlendirilmiş bir mesaj elde edilmiştir.

From::sip:kubra@voip.com

Alan Değeri Hataları: SIP mesajlarında bazı alanlar, belirli aralıklarda tanımlanan değerlere sahiptirler. Saldırgan, hatalı biçimlendirilen mesajlar üretmek için bu tanımlı aralığın üstünde ya da altında değerler kullanabilir. Alt sınırı 0, üst sınırı 255 olarak tanımlanan Max-Forward alanı için bu aralığın dışında bir değer verilmesi sağlanarak, standart olmayan bir mesaj üretilebilir.

Max-Forward:8888

2.4.GÜVENLİK YÖNTEMLERİ

VoIP teknolojisinde iletişim, gerçek zamanlı olarak ve internet altyapısı üzerinden gerçekleşmektedir. İnternet üzerinden hizmet veren diğer servisler gibi VoIP teknolojisi de çeşitli saldırıların hedefi haline gelmiştir. Bu saldırılar sonucunda, hedef sisteme kısa bir süreliğine erişilememesi durumunda bile veri kayıplarının yaşanması kaçınılmaz olacaktır. Hizmet kesintisi yaşandığında, kesinti boyunca gönderilen veri paketleri ve mesajlar iletilmez. Gönderilen paketler herhangi bir yerde saklanmadığı için tekrar gönderilmesi söz konusu olmayacaktır.

VoIP/SIP teknolojisini hedef alan saldırıların etkilerini en aza indirgemek ya da saldırıların etkilerini tamamen yok edebilmek için geliştirilmiş çeşitli güvenlik yöntemleri ve protokoller bulunmaktadır. Geliştirilen bu güvenlik yöntemleri ve protokoller ile kullanıcılara yüksek hizmet kalitesi sunulması ve kullanıcılar arasında veri güvenliğinin sağlanması hedeflenmektedir.

2.4.1. Şifreleme Yöntemleri

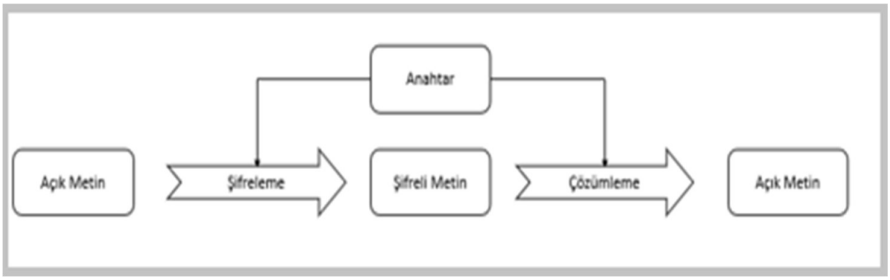
Şifreleme, sisteme tanımlı olan kullanıcılar arasında iletilecek verilerin gizliliğini ve bütünlüğünü sağlamak amacıyla verilerin gizlenmesi ve çözümlenmesi işlemidir. Şifreleme ile iletilecek veri paketlerine yalnızca ilgili kişilerin erişebilmesi sağlanır. Verilerin kullanıcılar arasında güvenli bir şekilde iletilmesini sağlayan şifreleme mekanizmalarında, şifreleme ve

çözümleme olmak üzere iki farklı algoritma kullanılır. Kullanıcılar arasında iletilmek istenen mesajın orijinal hali açık metin (plain text) olarak adlandırılırken, bu mesajın şifrelenmiş hali ise şifreli metin (chipered text) olarak adlandırılmaktadır.

Şekil 2.9: Şifreleme mekanizması [31].

Kullanıcılar arasında şifrelenmiş mesajlar gönderilerek, saldırganların orijinal mesaj içeriğine erişmesi engellenebilir. Şifreleme yöntemleri, simetrik ve asimetrik şifreleme algoritmaları olmak üzere iki başlık altında incelenmektedir [31,32].

Simetrik Şifreleme Algoritmaları: Simetrik şifrelemede, şifreleme ve deşifreleme işlemleri için tek bir anahtar kullanılmaktadır. Şifreleme ve çözümleme işlemleri sırasında kullanılan bu anahtar, sadece gönderici ve alıcı tarafından bilinmektedir. Anahtar, iletişim kurulmadan önce gönderici ve alıcı arasında güvenli bir şekilde iletilmektedir. Simetrik şifreleme algoritmalarına örnek olarak DES, 3DES ve AES algoritmaları verilebilir.



Şekil 2.10: Simetrik şifreleme mekanizması.

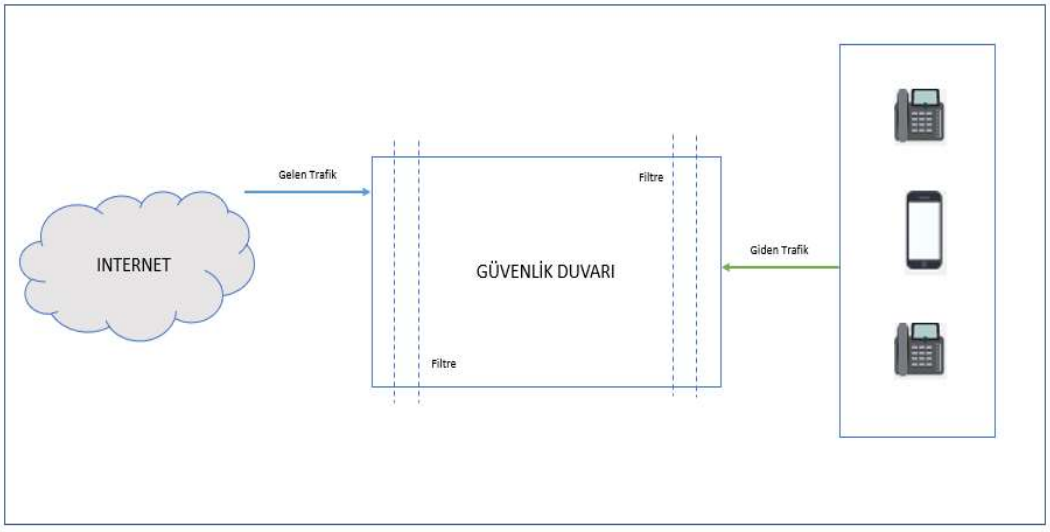
Asimetrik Şifreleme Algoritmaları: Asimetrik şifrelemede, şifreleme ve deşifreleme işlemleri için farklı iki anahtar kullanılmaktadır. Şifreleme işlemi, herkes tarafından bilinen ya da kolayca tahmin edilebilen açık anahtar ile yapılırken; şifre çözümleme işlemi yalnızca alıcı tarafından bilinen gizli anahtar ile yapılmaktadır. Kullanılan açık ve gizli anahtarlar, her oturum için farklı olarak üretilir yani bu anahtarlar kullanıcıya özeldir. Asimetrik şifreleme algoritmalarına örnek olarak Diffie-Helman ve RSA algoritmaları verilebilir.

Şekil 2.11: Asimetrik şifreleme mekanizması.

2.4.2. Güvenlik Duvarı

Güvenlik duvarı, ağ trafiğinin izlenmesini ve güvenlik zafiyetlerine karşı hedef sistemin korunmasını sağlayan yazılım ya da donanım tabanlı ağ geçidi çözümüdür. Yerel ağ üzerinde bulunan kaynakların, iç ve dış ağlar üzerinden gelebilecek saldırılara karşı korunmasını sağlayan ve dış ağlar üzerinde yer alan kaynaklara erişilmesini sağlayan önemli bir güvenlik mekanizmasıdır.

Güvenlik duvarı, genellikle yerel ağ ve internet çıkışı arasında konumlandırılmaktadır. Bu sayede ağ üzerinde iletilen tüm paketler güvenlik duvarı üzerinden geçmekte ve analiz edilmektedir. İç ve dış ağlar arasında oluşan trafiği denetlemek amacıyla güvenlik duvarı üzerinde kural tanımlamaları yapılmaktadır. Tanımlanan kurallar sayesinde, ağ üzerinde hangi paketlerin geçirileceğine, hangi paketlerin düşürüleceğine karar verilir.



Şekil 2.12: Güvenlik duvarı çalışma mimarisi.

Güvenlik duvarı üzerinde kaynak IP adresleri, hedef IP adresleri ve port numaraları belirtilerek kural tanımlamaları yapılmaktadır. Kural tanımlaması yapılırken, dış ağ üzerinde yer alan bazı IP adreslerine erişim kısıtlaması getirilebilir ya da bazı IP adresleri engellenebilir [33].

2.4.3. IPSec

Internet Protocol Security (IPSec, Internet Protokolü Güvenliği), ağ katmanı üzerinde veri güvenliğinin sağlanması için geliştirilmiş bir standarttır. Güvenli ağ kavramının oluşturulması amacıyla ağ katmanında iletilen verinin tünellenmesini ve şifrelenmesini sağlamaktadır. IPSec mimarisi temelinde ESP ve AH protokollerini barındırmaktadır. Barındırdığı bu protokoller ile kimlik doğrulama ve veri bütünlüğünün yanı sıra, tekrarlama saldırılarına karşı da koruma sağlamaktadır.

IPSec mimarisinde, ulaşım ve tünel modu olmak üzere iki farklı mod kullanılmaktadır. Ulaşım modu, yalnızca veri şifreleme için kullanılır iken; ulaşım moduna göre daha güvenli olan tünel modu ise veri ve paket başlığı şifreleme için kullanılmaktadır [34].

2.4.4. TLS

Transport Layer Security (TLS, Taşıma Katmanı Güvenliği), ulaşım katmanında güvenliğin sağlanması için geliştirilmiş bir protokoldür. Genellikle güvenli bağlantıların kurulması için kullanılan bu protokol, sadece TCP protokolü ile çalışmaktadır. TLS mimarisi temelinde, TLS kayıt protokolünü ve TLS el sıkışma protokolünü barındırmaktadır. El sıkışma protokolü, güvenlik parametrelerinin belirlenmesi ve katılımcı kimliklerinin doğrulanması için kullanılmaktadır. Kayıt protokolü ise, katılımcılar arasında iletilecek verinin gizliliğini ve bütünlüğünü sağlamak için kullanılmaktadır [35].

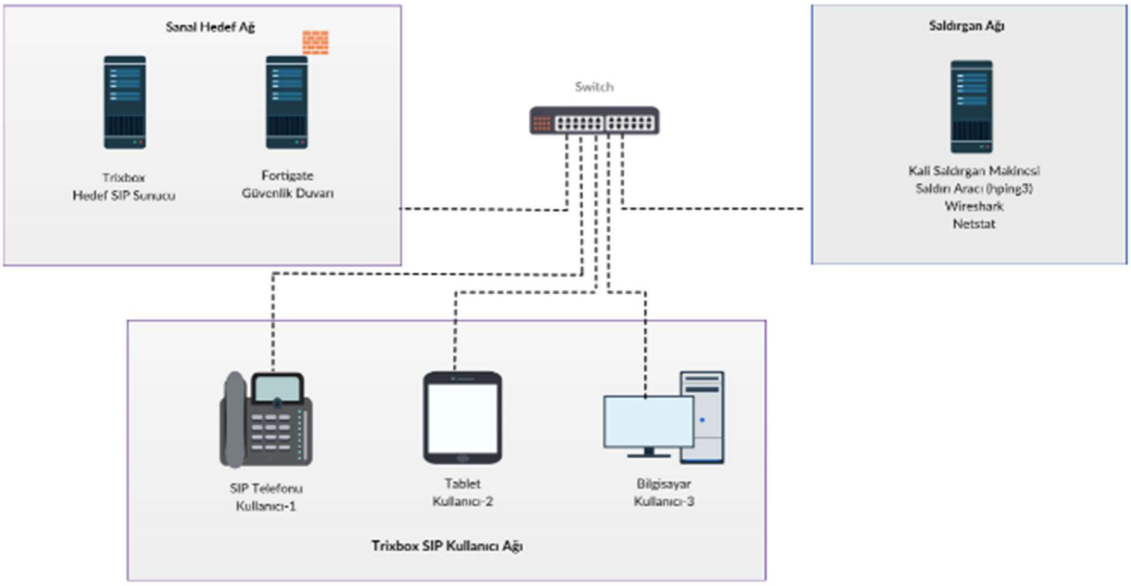
2.4.5. SRTP

Secure Real Time Transport Protocol (SRTP, Güvenli Gerçek Zamanlı Aktarım Protokolü), VoIP mimarisi için geliştirilmiş bir protokoldür. SRTP, RTP ve RTCP paketlerinin şifrelenmesini ve bu paketlerin bütünlüğünü sağlayarak; bileşenler arasında gerçek zamanlı olarak sorunsuz bir şekilde iletilmesini sağlamaktadır [36].

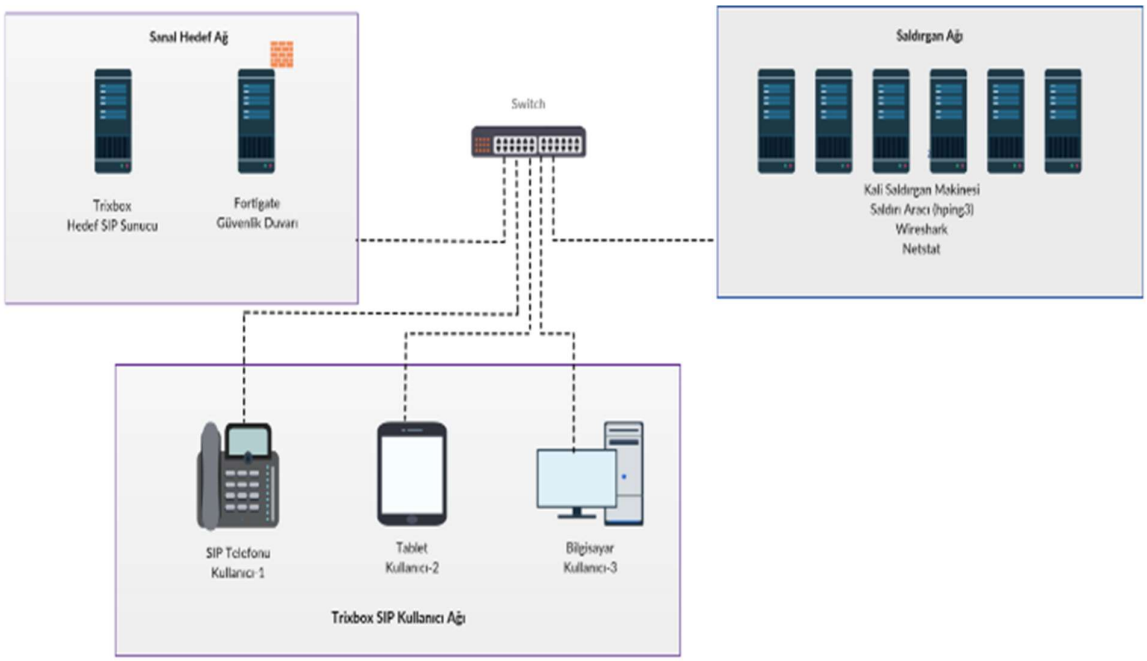
3. MALZEME VE YÖNTEM

3.1.VOIP/SIP GÜVENLİK LABORATUVAR ORTAMI

Bu tez çalışmasında, VoIP/SIP sistemlerinin güvenlik zafiyetlerinin belirlenebilmesi ve sistemlerin olası bir saldırı karşısında duyarlılıklarının ölçümlenebilmesi için Şekil 3.1'deki ve Şekil 3.2'deki gibi iki farklı laboratuvar ortamı oluşturulmuştur. Oluşturulan laboratuvar ortamlarında, kurumsal bir haberleşme ortamının yansıtıldığı VoIP ağı üzerinde; SIP sinyalleşme protokolü ile kullanıcıların kayıt olma, oturum başlatma ve oturum sonlandırma adımları gerçekleştirilmiştir. Sonrasında laboratuvar ortamlarında yer alan çeşitli yazılımlar ve araçlar kullanılarak, SIP sunucusunun kaynaklarını tüketmeye yönelik ve hizmet vermesini engellemeye yönelik flood tabanlı DoS ve DDoS saldırı senaryoları gerçekleştirilmiştir. Hazırlanan saldırı simülasyonları ilk olarak, herhangi bir güvenlik mekanizmasına sahip olmayan bir sistem üzerinde gerçekleştirilmiş ve etkileri gözlemlenmiştir. Daha sonra oluşturulan iki farklı laboratuvar ortamında, güvenlik duvarı konumlandırılmış ve saldırı simülasyonları tekrarlanmıştır.



Şekil 3.1: VoIP/SIP güvenlik laboratuvar ortamı-1.



Şekil 3.2: VoIP/SIP güvenlik laboratuvar ortamı-2.

Oluşturulan VoIP/SIP güvenlik laboratuvar ortamlarında kullanılan yazılımlar ve uygulamalar aşağıda açıklanmıştır.

Virtualbox: Kullanıcılara, mevcut fiziksel kaynakları üzerinde birden fazla ve farklı işletim sistemi çalıştırabilme olanağı sağlayan bir sanallaştırma yazılımıdır. Bu yazılım, x86 tabanlı ve x64 tabanlı bilgisayarlar üzerinde sanallaştırma altyapısının oluşturulmasını sağlar. Birden çok platform ve işletim sistemi tarafından desteklenen Virtualbox, yüksek bir kullanım oranına sahiptir. Laboratuvar ortamlarında, kullanılan bilgisayarların sanallaştırılması için Virtualbox yazılımı tercih edilmiştir [37].

Asterisk: Kullanıcılara, mevcut fiziksel kaynaklarını, bir haberleşme sunucusu gibi çalıştırabilme olanağı sağlayan açık kaynak kodlu bir PBX yazılımıdır. Linux, BSD, MacOSX gibi birçok işletim sistemi tarafından desteklenmesi ve ücretsiz bir yazılım olması nedeniyle popüler PBX yazılımları arasında yer almaktadır. İşletmeler, çağrı merkezleri, santraller ve devlet kurumları tarafından tercih edilen bu yazılım ile IP telefonlar arasında eş zamanlı çağrıların oluşturulması, çağrıların yönlendirilmesi ve çağrı kayıtlarının tutulması gibi birçok işlem gerçekleştirilmektedir [38].

Trixbox: Asterisk tabanlı bir PBX yazılımıdır. Başlangıçta Asterisk@Home adı ile yayınlanmıştır. Ancak 2006 yılında Digium firması tarafından yapılan değişiklik ile Trixbox adı altında hizmet vermeye başlamıştır. Trixbox sahip olduğu web arayüzü ile kullanıcılarına; kurulum, yönetim ve kullanım kolaylığı sağlamaktadır. Hazırlanan saldırı simülasyonları için SIP-PBX sistemi olarak Trixbox kullanılmıştır [39].

Kali Linux: Güvenlik zafiyet analizi için geliştirilen Kali Linux, Debian tabanlı bir Linux dağıtımıdır. Backtrack işletim sisteminin devamı niteliğinde geliştirilmiş bu yazılımın içerisinde; ağ üzerindeki güvenlik açıklarının tespit edilmesini sağlayan birçok uygulama ve araç bulunmaktadır. İçerisindeki bu uygulamalar ve araçlar kullanım amaçlarına göre sınıflandırılmış ve çeşitli kategoriler altında toplanmıştır. Bu sayede kullanıcılara, gerçekleştirecekleri sızma (penetrasyon) testleri için kullanım kolaylığı sağlanmıştır. Oluşturduğumuz laboratuvar ortamlarında, flood tabanlı DoS ve DDoS saldırı senaryolarını gerçekleştirmek için Kali Linux yazılımı kullanılmıştır [40].

Wireshark: Ağ trafiğinin analiz edilmesini sağlayan ücretsiz bir yazılımdır. Wireshark, ağ içerisinde iletilen veri paketlerinin yakalanmasını, ilgili paketlerin incelenmesini ve bu paketler hakkında bilgi verilmesini sağlamaktadır. Ağ içerisinde iletilen veri paketlerinin, bir grafik arayüzü üzerinden izlenmesini ve incelenmesini sağlayan bu yazılım ile hem anlık ağ trafiği izlenebilir hem de daha önce kaydedilmiş ağ trafiğine ait dosyalar analiz edilebilir. Birden fazla protokolü yakalayabildiği ve inceleyebildiği için VoIP sızma testlerinde oldukça tercih edilen bir analiz yazılımıdır. Bu çalışmada, saldırı sırasında gönderilen paketlerinin yakalanması ve analiz edilmesi için Wireshark yazılımı kullanılmıştır. Wireshark üzerinde yalnızca istenen paketlerin görüntülenebilmesi için filtreleme özelliği kullanılmıştır [41].

Softphone: IP telefon mantığı ile çalışan bir yazılımdır. Softphone, bir PBX ya da SIP sağlayıcısı üzerinden çağrı yeteneklerinin kullanılmasını sağlamaktadır. Zoiper, X-Lite ve Blink yaygın olarak kullanılan softphone uygulamaları arasında yer almaktadır. Bu uygulamalar, internet üzerinden ücretsiz olarak indirilebilir ve son kullanıcı cihazları üzerinde VoIP görüşmeleri gerçekleştirmek için kullanılabilir. Laboratuvar ortamlarımızda, Trixbox SIP sunucusuna kayıtlı kullanıcılar için X-Lite uygulaması kullanılmıştır [42].

Zenmap: Güvenlik tarayıcısı olarak tasarlanan nmap yazılımına, grafiksel kullanıcı arayüz özelliğinin eklenmesi ile geliştirilen bir uygulamadır. Zenmap ile ağ taraması yapılarak, taranan

ağa ait bir harita oluşturulmaktadır. Oluşturulan bu harita sayesinde, ağda bulunan mevcut cihazların tespit edilmesi ve cihazlar üzerinde çalışan servislerin durumları, işletim sistemleri ve port durumları izlenebilir. Hedef IP aralığı belirtilerek, tarama işlemi başlatılır. Böylece belirtilen IP aralığında çalışan cihazlar gözlemlenebilir. Bu çalışmada, hedef olarak seçilen sistemin açık port ve kaynak bilgilerine ulaşmak için Zenmap kullanılmıştır [43].

Ngrep: Linux tabanlı sistemlerde içerik aramak için kullanılan grep komutunun ağ trafiği üzerinde kullanılması için geliştirilmiş halidir. Ağ trafiğini oluşturan veri paketlerinin izlenmesini, analiz edilmesini ve bu paketler içerisinde çeşitli ifadeler için arama yapılmasını sağlayan bir yazılımdır. Ngrep, sunucu ve istemci arasındaki ilgili trafiğin incelenerek, meydana gelen herhangi bir anormalliğin tespit edilmesini sağlamaktadır. IP, TCP, UDP, ICMP, IGMP protokollerini tanımaktadır ve filtreleme mantığını desteklemektedir. Bu sayede kaynak, hedef, protokol, port gibi değişkenler özel olarak seçilebilmekte ve filtreleme yapılan ağ trafiği üzerinde çeşitli ifadeler için arama yapılabilmektedir [44].

Netstat: Unix, Linux ve Windows tabanlı sistemlerde ağ trafiğinin anlık olarak kontrol edilmesini sağlamak amacıyla kullanılan bir komut satırı aracıdır. Komut satırı üzerinden ağ bağlantılarının, yönlendirme tablolarının ve ağ arabirim istatistiklerinin gözlemlenmesini sağlamaktadır. Bu çalışmada, SIP sunucusuna gelen bağlantıların ve ağ paket sayısı istatistiklerinin izlenebilmesi için netstat komutu kullanılmıştır.

Htop: Unix ve Linux tabanlı sistemlerde kullanılan top komutuna alternatif olarak geliştirilen htop, sistem süreçlerinin gerçek zamanlı olarak izlenmesini sağlayan bir süreç görüntüleme yazılımıdır. Bir bilgisayar ya da makine üzerinde çalışan süreçlerin, CPU kullanım oranlarına göre sıralanmasını, listelenmesini ve bu listelerin sık aralıklarla güncellenerek konsol ekranında görüntülenmesini sağlar. Bu çalışmada, flood tabanlı DoS ve DDoS saldırıları sonucu tüketilen sistem kaynaklarına ait sonuçların elde edilmesi ve karşılaştırma yapılması için htop aracı kullanılmıştır [45].

Vmstat: Linux tabanlı sistemlerde makine üzerindeki sanal bellek kullanımına ilişkin ayrıntılı bilgi edinmek amacıyla kullanılan bir konsol komutudur. Vmstat komutu ile belirli zaman aralıkları ile bellek kullanımına dair ayrıntılı istatistiksel raporlar hazırlanabilir ve bu raporlar belirli zaman aralıkları ile ekrana sürekli yansıtılabilir. Bu çalışmada, flood tabanlı DoS ve

DDoS saldırıları sonucu tüketilen sistem kaynaklarına ait sonuçların elde edilmesi ve karşılaştırma yapılması için vmstat aracı kullanılmıştır [46].

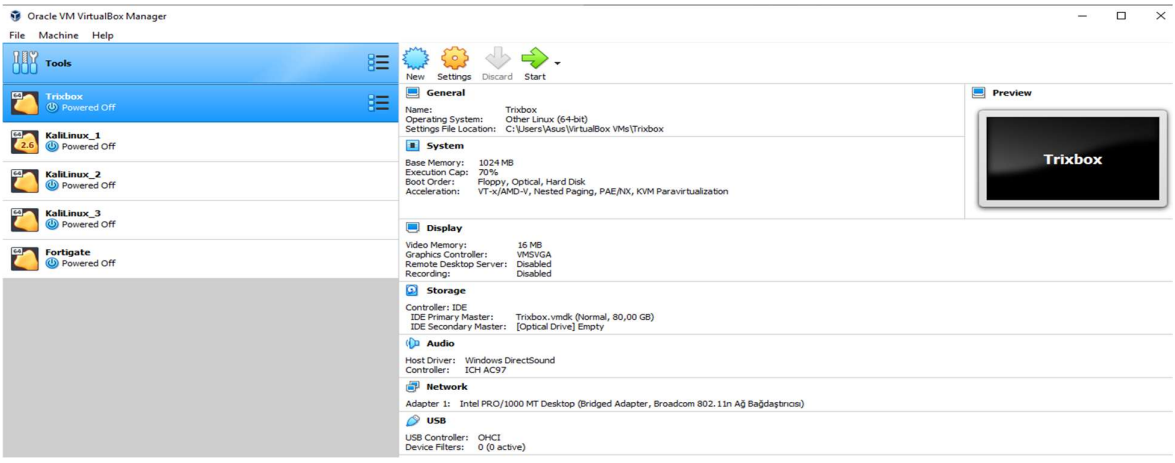
Fortigate: Ağ üzerindeki anomalilerin tespit edilebilmesi, olası saldırıların algılanabilmesi ve saldırıların önlenebilmesi amacıyla Fortinet firması tarafından geliştirilmiş ücretli bir güvenlik duvarı yazılımıdır. Yaygın olarak büyük ölçekli şirketler ve servis sağlayıcılar tarafından kullanılan bu yazılım ile IP ağları üzerinde gerçek zamanlı olarak trafik analizi ve paket izlemesi yapılarak, saldırı tespiti gerçekleştirilebilir ve tespit edilen saldırıları engellemek amacıyla çeşitli kurallar oluşturulabilir. Bu çalışmada, SIP sunucusuna yönelik saldırıları tespit edebilmek ve rate limiting tabanlı saldırı engelleme kurallarının uygulanması için Fortigate yazılımı tercih edilmiştir [47].

3.2.LABORATUVAR ORTAMLARININ KURULUMU VE YAPILANDIRILMASI

Bu bölümde, VoIP/SIP güvenlik laboratuvar ortamlarının oluşturulması için gerekli olan yazılımların ve uygulamaların, kurulum ve yapılandırma aşamalarına değinilmiştir.

3.2.1. Trixbox PBX Kurulumu ve Yapılandırılması

Güvenlik laboratuvar ortamlarının hazırlanması sırasında, Virtualbox yazılımı üzerine sanal SIP-PBX sistemi olarak çalışacak Trixbox sistemi kurulmuştur. Kurulum tamamlandıktan sonra, varsayılan "root" kullanıcı yetkisinde, komut satırı üzerinden yönetim sağlanmaktadır.



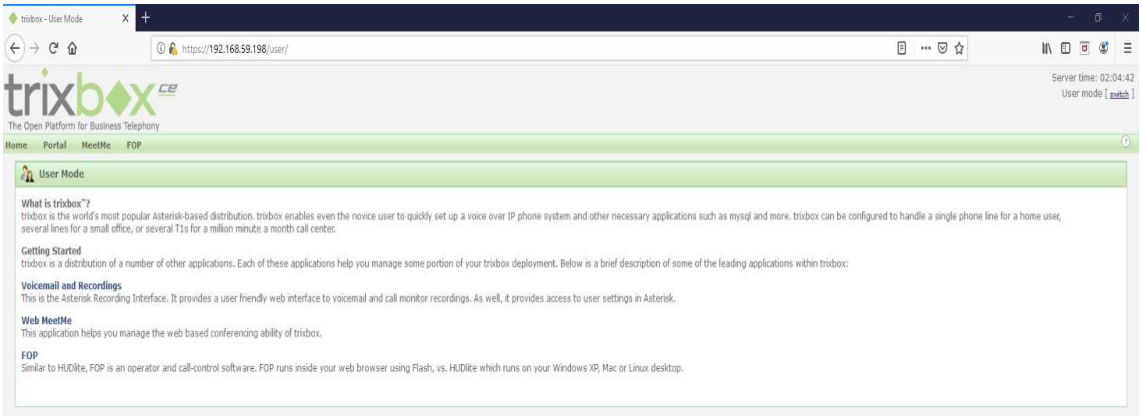
Şekil 3.3: Laboratuvar ortamının Virtualbox üzerinde kurulumu.

Trixbox kurulumu sırasında, IP adresi DHCP üzerinden otomatik olarak dağıtılmıştır. Linux tabanlı sistemlerde kullanılan “ifconfig” komutu ile Şekil 3.4’te gösterildiği gibi Trixbox SIP sunucusuna otomatik olarak atanan IP adresi belirlenmiştir. Belirlenen IP adresi herhangi bir internet tarayıcısına yazılarak, SIP-PBX sistemine web arayüzü üzerinden erişim sağlanmıştır. Web arayüzüne erişim varsayılan olarak, “User” yetkisi ile sağlanmaktadır. Sistemde tanımlı olan kullanıcı adı ve şifre bilgilerinin (varsayılan olarak maint/password) girilmesinin ardından sağ üst köşede yer alan kullanıcı değiştirme butonu kullanılarak, “Admin” yetkisine geçiş sağlanmaktadır.

```
[trixbox1.localdomain ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:4C:26:74
          inet addr:192.168.59.198  Bcast:192.168.59.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4c:2674/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2457 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2250 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:283749 (277.0 KiB)  TX bytes:1746633 (1.6 MiB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:927 errors:0 dropped:0 overruns:0 frame:0
          TX packets:927 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:75305 (73.5 KiB)  TX bytes:75305 (73.5 KiB)
```

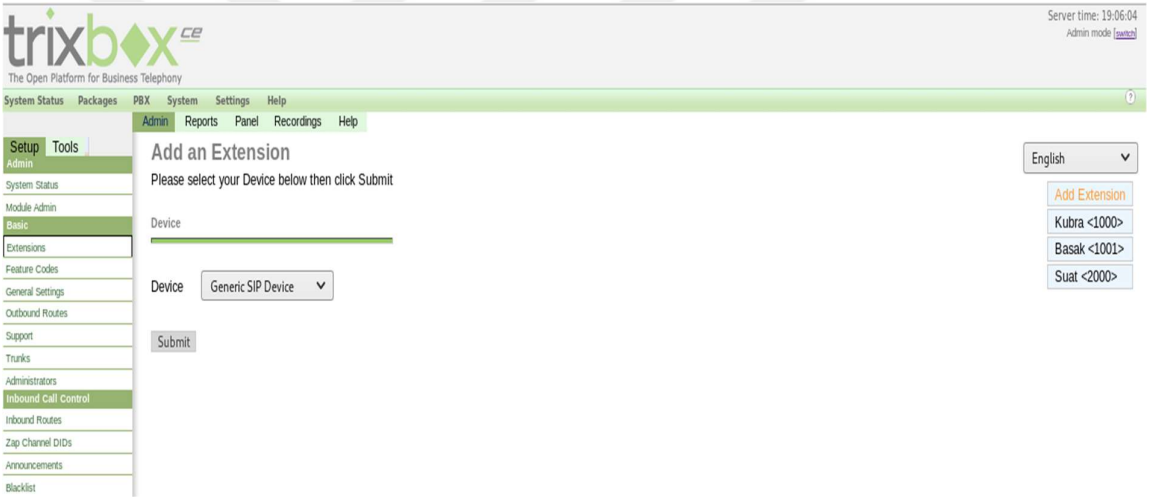
Şekil 3.4: Trixbox IP adresinin ifconfig komutu ile belirlenmesi.



Şekil 3.5: Trixbox’ın web arayüzü üzerinden ilk açılış ekranı.

İstemci-sunucu mimarisine göre tasarlanan laboratuvar ortamlarımızda, istemci rolündeki SIP kullanıcılarının tanımlanabilmesi için Şekil 3.6'daki gibi çeşitli dahili kullanıcılar oluşturulmuş ve her dahili kullanıcı için farklı kullanıcı adı ve şifre tanımlamaları yapılmıştır. Bu sayede, kullanıcıların aynı ağ üzerinde herhangi bir fiziksel kaynak üzerine kurulmuş olan istemci yazılımları ile SIP-PBX sunucusu üzerine kayıt olmaları sağlanmıştır. Trixbox için varsayılan sinyalleşme protokolü SIP protokolüdür ancak farklı sinyalleşme protokolleri de desteklenmektedir.

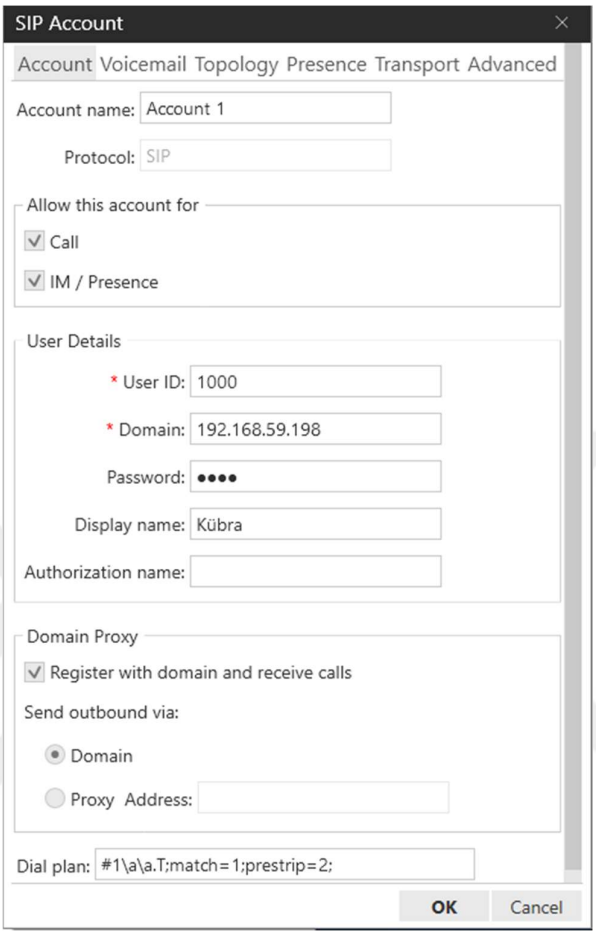
Bu çalışmada, saldırı simülasyonlarını gerçekleştirmek için 1000, 1001 ve 2000 numaralarına sahip kullanıcı tanımlamaları yapılmıştır.



Şekil 3.6: Trixbox dahili kullanıcı oluşturma ekranı.

3.2.2. Softphone Kurulumu ve Yapılandırması

Hazırlanan güvenlik laboratuvar ortamlarında, SIP-PBX sunucusuna kayıtlı olan kullanıcıların birbirleri ile iletişim kurabilmeleri için ilgili istemci yazılımlarının aynı ağ üzerinde herhangi bir fiziksel kaynak üzerine kurulması ve yapılandırılması gerekir. Bir fiziksel kaynak (kişisel bilgisayar, dizüstü bilgisayar, akıllı telefon, vb.) üzerine kurulumları yapılan istemci yazılımları için sinyalleşme protokolü olarak SIP seçilir. SIP-PBX sunucusuna kayıtlı olan dahili kullanıcıların, kendilerine ait kullanıcı adı ve şifre bilgilerine ek olarak SIP sunucusuna ait IP adresini etki alanı (domain) olarak belirtmesi ile istemci yazılımlarının Trixbox sistemi üzerine kaydedilmesi sağlanmaktadır. Bu çalışmada, istemci yazılımı olarak kullanılan X-Lite programı üzerinde gerçekleştirilen kullanıcı kayıt işlemlerinin bir örneğine Şekil 3.7'de yer verilmiştir.



Şekil 3.7: X-Lite soft phone uygulaması ile kayıt olan kübra kullanıcısı.

3.2.3. Kali Linux Kurulumu ve Yapılandırılması

Hazırlanan iki farklı güvenlik laboratuvar ortamında, saldırı simülasyonlarının gerçekleştirilebilmesi için saldırgan makine rolünde kullanılan Kali Linux işletim sistemi, Virtualbox üzerine kurulmuştur ve sanal olarak çalıştırılmıştır. Kali Linux'un kurulumu esnasında, IP adresi DHCP üzerinden otomatik olarak dağıtılmıştır.

Kali Linux işletim sistemi içerisinde bulunan uygulamalar ve araçlar, terminal komut satırı üzerinden ya da kullanıcı arayüzü üzerinden çalıştırılabilir. Bu uygulamalar ve araçlar kullanılarak hedef olarak belirlenen bir sistemin güvenlik zafiyetleri tespit edilebilir ve çeşitli saldırılar gerçekleştirilebilir. Şekil 3.8'de Kali Linux sistemi üzerinde bulunan uygulamaların ve araçların amaçlarına göre sınıflandırılarak, çeşitli kategoriler altında toplandığı gösterilmiştir.

Şekil 3.8: Kali Linux uygulamalar ve araçlar ekranı.

3.2.4. Fortigate Kurulumu ve Yapılandırması

Oluşturulan güvenlik laboratuvar ortamlarında, ağ üzerindeki anomalileri tespit edebilmek ve engelleyebilmek amacıyla Virtualbox üzerine Fortigate kurulumu gerçekleştirilmiş ve sanal olarak çalıştırılmıştır. Fortigate kurulumu sırasında, IP adresi DHCP üzerinden otomatik olarak dağıtılmaz. Bu nedenle, kurulum sonrasında interface (arayüz) yapılandırmaları manuel olarak yapılmıştır. Bu çalışmada, hedef olarak belirlenen SIP-PBX sunucusu ve saldırgan makine/makineler arasında konumlandırılan güvenlik duvarı için iki farklı arayüz tanımlaması yapılmıştır. Tanımlanan ilk arayüz SIP-PBX sunucusunun varsayılan ağ geçidi olarak yapılandırılmış, ikinci arayüz ise saldırgan makine/makinelerin varsayılan ağ geçidi olarak yapılandırılmıştır.

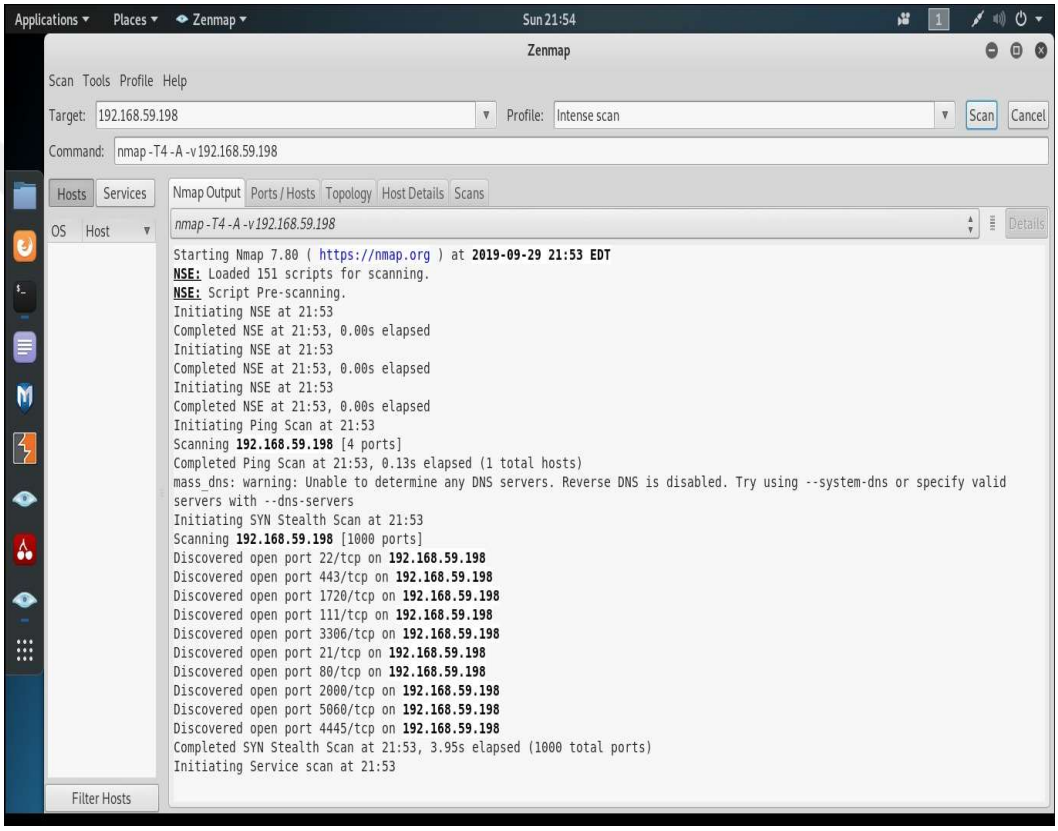
Status	Name	Members	IP/Netmask	Type	Access
Physical (10)					
	port1 (TRIX)		192.168.59.2 255.255.255.0	Physical Interface	PING HTTPS HTTP
	port2 (KALI)		192.168.60.2 255.255.255.0	Physical Interface	PING HTTPS SSH

Şekil 3.9: Fortigate arayüz yapılandırmaları.

3.3.VOIP SİSTEMLERİNİN KEŞFEDİLMESİ

Yerel ağ üzerinde bulunan VoIP sistemlerinin tespit edilebilmesi için çeşitli yöntemler geliştirilmiştir. Port tarama, hedef sistemlerin keşfedilmesinde yaygın olarak kullanılan

yöntemler arasında gösterilmektedir. Bu çalışmada, SIP sunucusuna ilişkin bilgi edinebilmek amacıyla Kali Linux işletim sistemi üzerinde bulunan Zenmap uygulaması kullanılmıştır. Zenmap uygulaması ile port tarama işlemi gerçekleştirilmiş ve hedef olarak belirlenen sistemin açık olan portlarına ilişkin bilgi toplanmıştır. Şekil 3.10'da görüleceği üzere, 192.168.59.198 IP adresi için sorgu yapıldığında; SIP-PBX sunucusuna ait açık port listesine ulaşılmıştır.



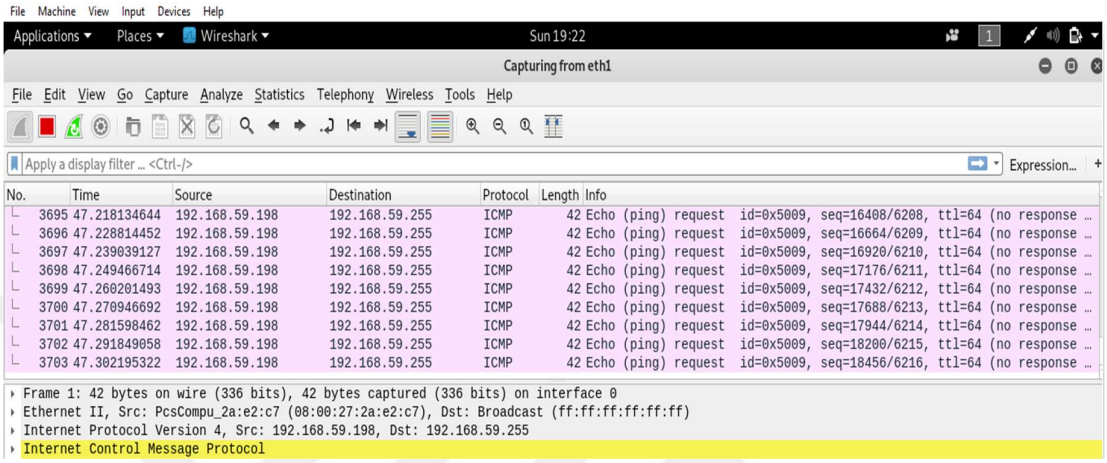
Şekil 3.10: Kali Linux üzerinde Zenmap ile port tarama.

3.4.VOIP TRAFİĞİNİN ANALİZ EDİLMESİ

Hazırlanan güvenlik laboratuvar ortamlarında, ağ analizi için Wireshark yazılımı kullanılmıştır. Bu sayede, ağ içerisinde iletilen veri paketlerinin yakalanması, ilgili paketlerin incelenmesi ve bu paketler hakkında bilgi edinilmesi sağlanmıştır.

Bu çalışmada, VoIP/SIP sistemlerine yönelik gerçekleştirilen flood tabanlı DoS ve DDoS saldırıları sırasında ağ içerisinde iletilen paketler incelenmiştir. Şekil 3.11'de Wireshark

yazılımının filtreleme özelliği kullanılarak, ICMP flood tabanlı bir DoS saldırısı esnasında ağın broadcast adresine gönderilen ICMP paketleri gösterilmektedir.

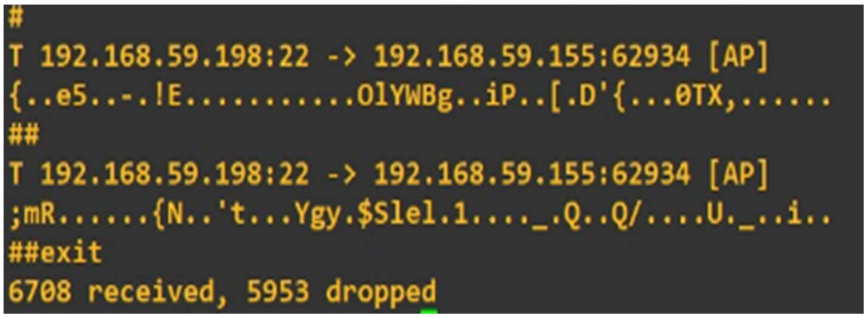


Şekil 3.11: Wireshark ile ICMP paketlerinin analiz edilmesi.

3.5.VOIP TRAFİĞİNİN İZLENMESİ

Oluşturulan laboratuvar ortamlarında, saldırgan makine/makineler olarak konumlandırılan Kali Linux işletim sistemleri ile gerçekleştirilen saldırılar sırasında, hedef olarak belirlenen SIP-PBX sunucusuna aynı anda çok sayıda paket gönderilmektedir.

Bir saldırı sırasında, SIP sunucusu rolündeki Trixbox üzerinde ngrep komutunun çalıştırılması ile sunucu üzerinden geçen tüm ağ trafiği izlenebilir. Güvenlik duvarının aktif edildiği bir saldırı senaryosu esnasında, "ngrep -W byline -d eth0" komutunun çalıştırılması ile Trixbox üzerinden geçen ağ trafiğine ilişkin bir kesit Şekil 3.12'de gösterilmiştir.



Şekil 3.12: Ngrep komutu ile ağ trafiğinin izlenmesi.

3.6.VOIP/SIP LABORATUVAR ORTAMLARINDA SALDIRI SENARYOLARININ GERÇEKLEŞTİRİLMESİ

VoIP mimarisinde ses, video, anlık mesajlaşma gibi çoklu ortam verilerinin iletimi IP ağı üzerinden sağlanmaktadır. IP protokol yapısında bulunan güvenlik zafiyetleri nedeniyle, VoIP sistemleri başta DoS/DDoS saldırıları olmak üzere çeşitli saldırıların hedefi haline gelmektedir. DoS/DDoS saldırıları, hizmet engellemeye yönelik saldırılardır. Bu saldırılar, hedef olarak belirlenen sistemin cevap veremeyeceği kadar çok istek paketinin gönderilmesi ve hedef sistemin bellek, işlemci, disk alanı ve bant genişliği gibi kaynaklarının tüketilmesi gibi farklı şekillerde gerçekleştirilir. DoS/DDoS saldırıları ile hedef sistemin geçici bir süreliğine ya da tamamen erişilemez hale getirilmesi amaçlanmaktadır.

Flood tabanlı DoS ve DDoS saldırılarında, hedef sisteme karşılayabileceğinden fazla paket gönderilir ve bu paketlerin işleme alınabilmesi için sistem kaynakları tüketilmeye başlanır. Oluşturulan ilk senaryoda, herhangi bir güvenlik mekanizmasına sahip olmayan bir sistem hedef alınarak, flood tabanlı çeşitli saldırılar ile sistem kaynakları tüketilmeye çalışılacak ve hizmet kesintilerinin yaşandığı gözlemlenecektir. Bir sonraki adımda ise, güvenlik duvarı ile korunan bir sistem hedef alınarak, flood tabanlı çeşitli saldırılar ile sistem kaynakları tüketilmeye çalışılacak ve hizmet kalitesinin korunduğu gözlemlenecektir.

3.6.1. UDP Flood Tabanlı DoS ve DDoS Saldırılarının Gerçekleştirilmesi

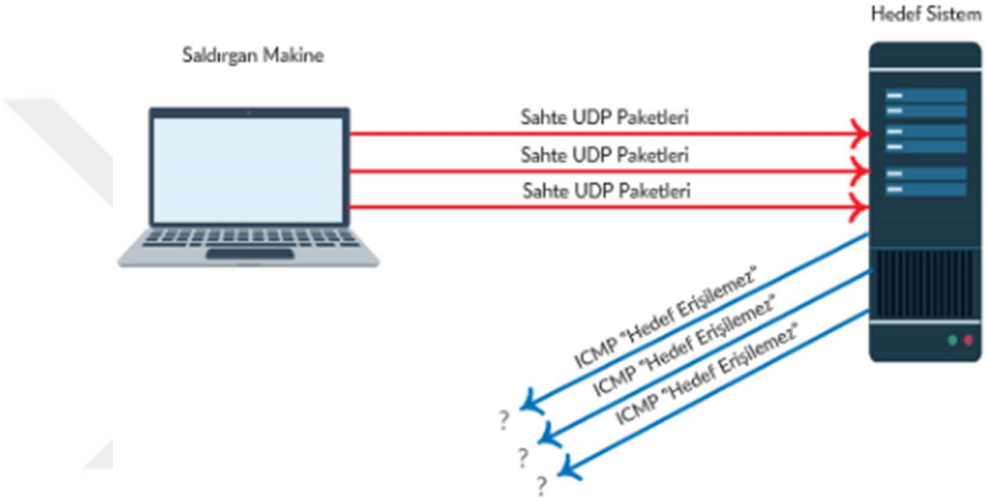
Hizmet engellemeye yönelik gerçekleştirilen UDP flood tabanlı DoS ve DDoS saldırılarında, hedef olarak belirlenen sisteme çok sayıda UDP paketi gönderilerek, sistemin bir süre sonra erişilemez hale getirilmesi amaçlanmaktadır.

SIP uygulamaları, QoS parametrelerine duyarlılıklarından ve zaman kritik olmalarından dolayı iletim protokolü olarak yaygın olarak UDP protokolünü kullanırlar. UDP protokolü yapısı gereği, veri paketlerinin ilgili alıcıya ulaşıp ulaşmadığını kontrol etmez. UDP flood tabanlı bir saldırı sırasında, hedef sistem kendisine gönderilen çok sayıdaki UDP paketlerinin her biri için aşağıdaki adımları gerçekleştirmeye çalışmaktadır.

- Hedef sistem, ilgili UDP portuna gelen trafiği dinleyerek, herhangi bir uygulamanın çalışıp çalışmadığını kontrol eder.

- Sistem, herhangi bir uygulamanın çalışmadığını tespit ettiğinde, hedefin erişilemez olduğunu belirtmek için ICMP “Destination Unreachable” paketi ile cevap verir.

Saldırı sırasında, yukarıdaki adımların gelen her bir UDP paketi için tekrarlanmaya çalışılması sonucunda, sistem kaynakları yetersiz kalmaya başlayacaktır ve sistem bir süre sonra hizmet veremez hale gelecektir.



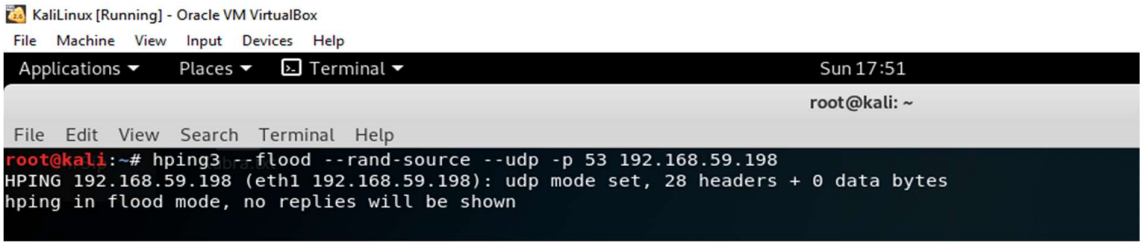
Şekil 3.13: UDP Flood tabanlı DoS saldırı senaryosu.

UDP flood tabanlı saldırılarda, saldırgan genellikle sahte IP adresleri kullanır. Bu sayede, saldırgan hem bağlantı konumunu gizlemiş olur hem de hedef sistem tarafından gönderilen “ICMP” cevap paketlerine maruz kalmamış olur.

Sahte IP adresleri kullanılarak, hedef olarak belirlenen bir SIP-PBX sunucusuna aynı anda çok sayıda UDP paketi gönderilmesi ile flood tabanlı DoS ve DDoS saldırıları gerçekleştirilmiştir. Bu saldırıların gerçekleştirilebilmesi için Kali Linux işletim sistemi içerisinde bulunan “hping3” isimli araçtan yararlanılmıştır.

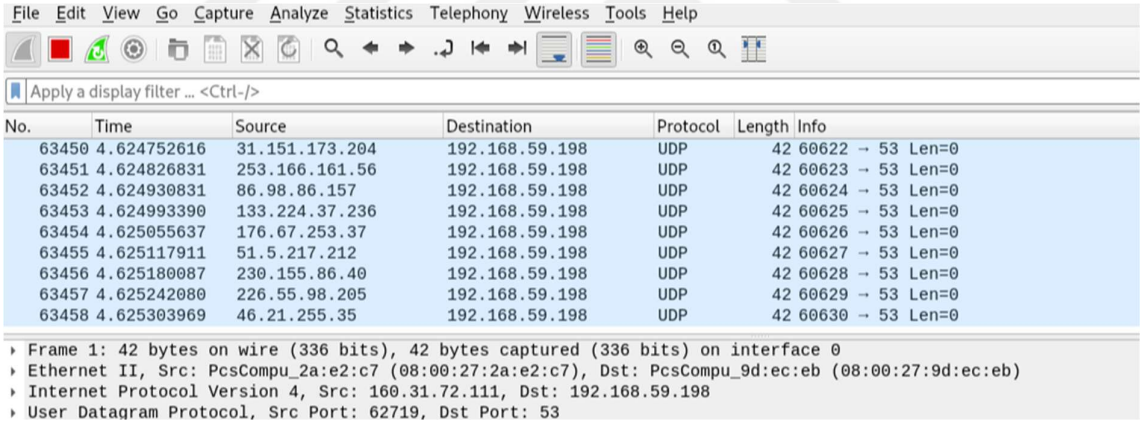
Saldırgan makine rolündeki Kali Linux işletim sistemi üzerindeki hping3 aracı ile 192.168.59.198 IP adresli Trixbox SIP sunucusunu hedef alan flood tabanlı saldırılar gerçekleştirebilmek amacıyla UDP paketleri gönderilir iken, çeşitli parametreler kullanılmaktadır. Şekil 3.14’de kullanılan parametreler incelendiğinde; sahte IP adresleri kullanılarak, hedef makinenin 53 numaralı portuna çok sayıda UDP paketinin gönderildiği

gösterilmiştir. Ek olarak kullanılan -- rand-source parametresi ile kaynak IP adresinin taklit edilmesi (spoof) ve her gönderilen paket için ayrı bir IP adresi kullanılması sağlanır.



Şekil 3.14: hping3 aracı ile UDP flood tabanlı DoS saldırısının başlatılması.

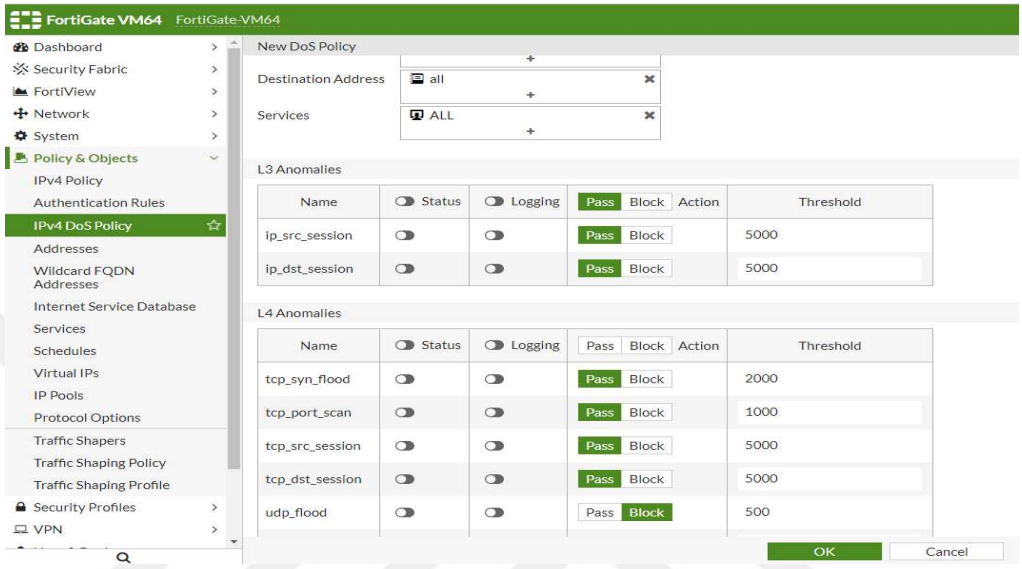
Saldırının gerçekleştiği sırada, hedef sunucuya kayıtlı olan 1000, 1001 ve 2000 kullanıcılarından herhangi birinin ekranı üzerinde Wireshark ağ analizi programı açılmış ve gelen UDP paketleri Şekil 3.15'deki gibi gözlemlenmiştir.



Şekil 3.15: Wireshark programı ile yakalanan UDP paketleri.

Saldırgan ya da saldırganlar tarafından hedef olarak belirlenen sisteme aynı anda çok sayıda UDP paketinin gönderilmesi ağ üzerinde bir anomali yaratır. Fortigate ile bu anomalilerin tespit edilebilmesi ve olası saldırılara karşı önlem alınabilmesi için çeşitli kurallar oluşturulabilir. Kural tanımlamaları yapılır iken, paket türü ve eşik değeri parametreleri dikkate alınır. Hedef sisteme iletilecek UDP paket sayısı için bir eşik değeri belirlenir. Sisteme gönderilmek istenen UDP paket sayısı, belirlenen eşik değerinden büyük ise; olası bir UDP flood tabanlı DoS/DDoS saldırısı olarak yorumlanır ve ilgili paketlerin hedef sisteme iletilmesi engellenir. Şekil 3.16'da hedef sisteme iletilmek istenen UDP paket sayısının 500'den fazla olması durumunda, olası bir

UDP flood saldırısı olarak algılanması ve iletilmek istenen paketlerin engellemesi için tanımlanan kural gösterilmiştir.



Şekil 3.16: Fortigate ile UDP flood tabanlı saldırılar için kural oluşturma.

Fortigate üzerinde gerçekleştirilen kural tanımlaması ile, ağ üzerinde UDP paketlerine ilişkin herhangi bir anomalinin tespit edilmesi durumunda alarm üretilmesi sağlanır. Ayrıca saldırı sırasında, Wireshark gibi ağ trafiği analiz araçları ile UDP tabanlı flood saldırılar manuel olarak da tespit edilebilmektedir. Ancak bu araçlar ile saldırı tespitinin yapılması belirli bir seviyede teknik anlamda uzmanlık gerektirmektedir.

3.6.2. SYN Flood Tabanlı DoS ve DDoS Saldırılarının Gerçekleştirilmesi

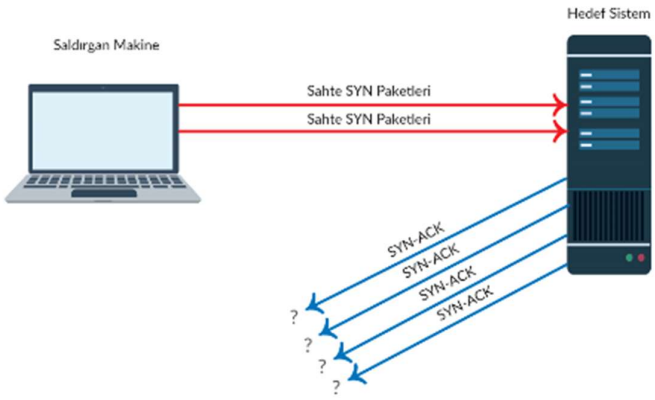
SYN flood tabanlı saldırılar, hizmet engelleme saldırıları arasında en sık karşılaşılan ve en kolay gerçekleştirilen saldırı türüdür. SYN flood tabanlı DoS/DDoS saldırılarında, hedef olarak belirlenen sisteme çok sayıda sahte SYN paketi gönderilerek, sistem kaynaklarının tüketilmesi ve sistemin hizmet veremez hale getirilmesi amaçlanır. Hedef sisteme gelen paket sayısı, sistemin karşılayabileceği paket sayısından fazla olduğunda; gelen paketlerin işleme alınabilmesi için sistem kaynakları kullanılmaya başlanır. Bunun sonucunda, sisteme kayıtlı gerçek kullanıcılar aynı anda hizmet isteğinde bulunduğunda, sistem bu isteklere cevap veremez hale gelecektir.

TCP protokolü yapısı gereği, veri paketlerinin kayıpsız ve denetimli olarak iletilmesini sağlar. İki kullanıcı arasında bir TCP bağlantısı kurulmak istendiğinde, TCP üçlü el sıkışma

mekanizması devreye girer. Bu sayede kullanıcılar arasında kayıpsız bir veri iletişimi sağlanır. TCP üçlü el sıkışma mekanizması için aşağıdaki adımlar uygulanır.

- A kullanıcısı, B kullanıcısına SYN paketi göndererek, bağlantı isteğinde bulunur.
- B kullanıcısı, kendisine gelen istek paketini aldığını belirtmek için ACK-SYN paketi gönderir.
- A kullanıcısı, B kullanıcısına ACK paketi gönderir ve bu paketin iletilmesi ile iki kullanıcı arasında TCP bağlantısı kurulmuş olur.

SYN flood tabanlı saldırılarda, sahte IP adresleri üzerinden, hedef olarak belirlenen sisteme çok sayıda SYN paketi gönderilir. Hedef sistem, kendisine gelen her SYN paketi için bir kaynak ayırır ve SYN-ACK paketi ile cevap döner. Sistem, bağlantının kurulduğuna dair kendisine, ACK paketinin gönderilmesi için bir süre bekler. Ancak bağlantı istekleri için sahte IP adresleri kullanıldığından, hedef sisteme bağlantı kurulduğuna dair ACK paketi gönderilmez. Sistem ACK paketini alamadığı için SYN-ACK paketini tekrar tekrar gönderir. Bu tekrarlama sonucunda, sistem kaynakları hızlı bir şekilde tükenmeye başlar ve sistem bir süre sonra hizmet veremez hale gelir.

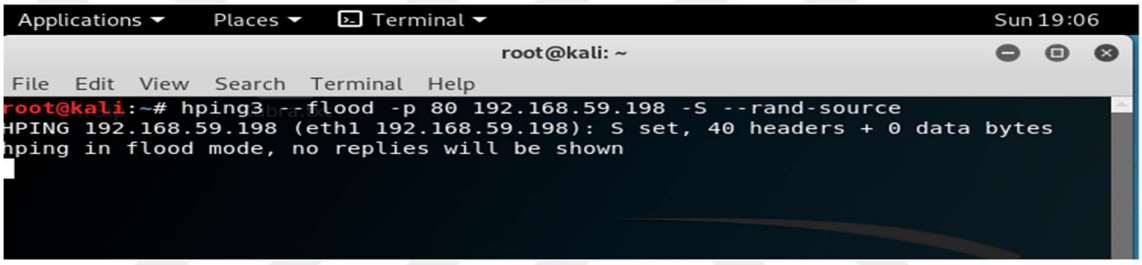


Şekil 3.17: SYN Flood tabanlı DoS saldırı senaryosu.

Sahte IP adresleri kullanılarak, hedef olarak belirlenen bir SIP-PBX sunucusuna aynı anda çok sayıda SYN paketi gönderilmesi ile flood tabanlı DoS ve DDoS saldırıları gerçekleştirilmiştir. Saldırı sırasında kullanılacak sahte IP adresleri saldırgan ya da saldırganlar tarafından manuel olarak belirlenebileceği gibi, istenilen sayı kadar random olarak da üretilebilir. Bu saldırıların

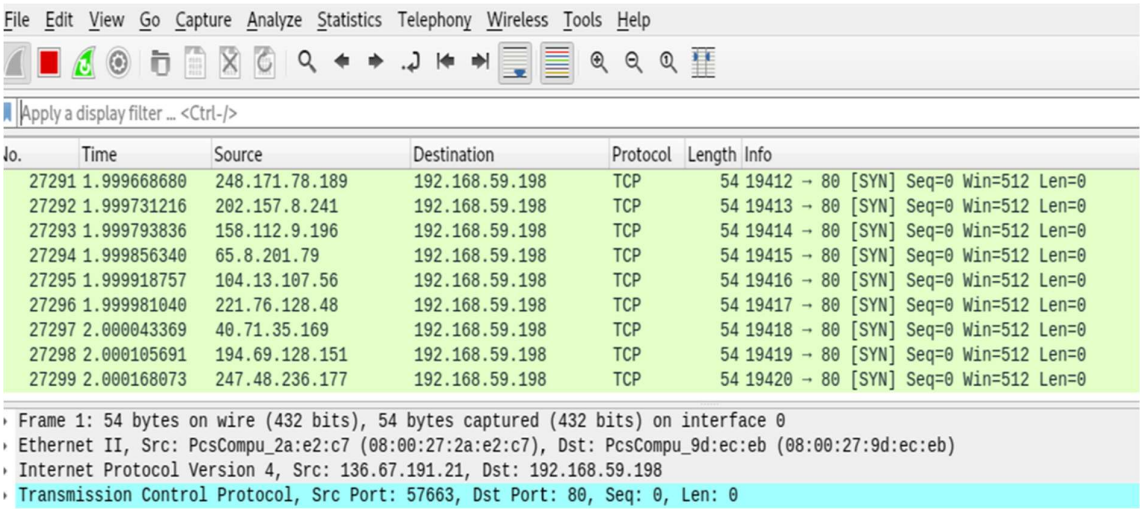
gerçekleştirilmesi için Kali Linux işletim sistemi içerisindeki "hping3" aracından faydalanılmıştır.

192.168.59.198 IP adresine sahip Trixbox SIP sunucusuna yönelik flood tabanlı saldırılar gerçekleştirebilmek için hping3 aracı ile birlikte çeşitli parametreler kullanılmaktadır. Şekil 3.18'de kullanılan parametreler incelendiğinde; sahte IP adresleri kullanılarak, hedef makinenin 80 numaralı portuna çok sayıda SYN paketinin gönderildiği gözlemlenmiştir. Saldırı sırasında kullanılan – rand-source parametresi ile gönderilen her bir SYN paketi için farklı bir IP adresi kullanılması sağlanmıştır.



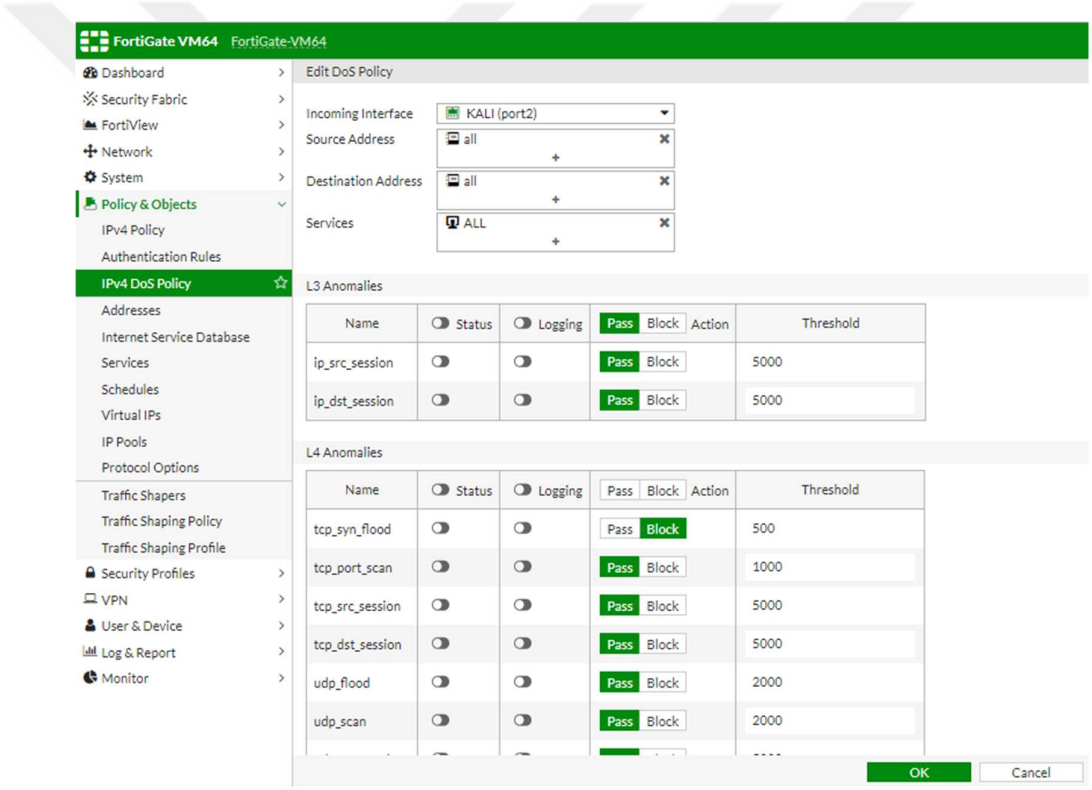
Şekil 3.18: hping3 aracı ile SYN flood tabanlı DoS saldırısının başlatılması.

Saldırılar esnasında, hedef SIP-PBX sunucusuna kayıtlı olan herhangi bir kullanıcı ekranı üzerinde Wireshark ağ analizi programı açılmış ve gelen SYN paketleri Şekil 3.19'daki gibi gözlemlenmiştir.



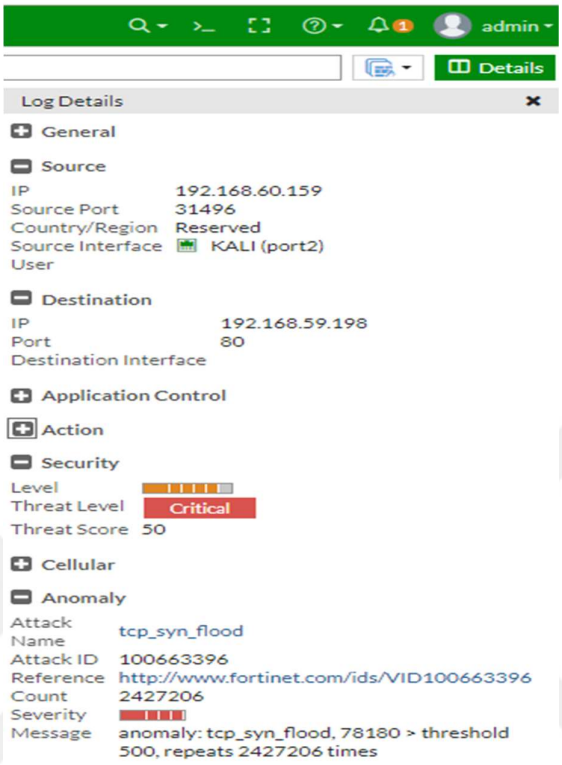
Şekil 3.19: Wireshark ile TCP-SYN paketlerinin yakalanması.

Bu tarz bir saldırının tespit edilebilmesi ve engellenebilmesi için Fortigate güvenlik duvarı kullanılabilir. Fortigate ile hedef sisteme, saldırgan ya saldırganlar tarafından aynı anda ve çok sayıda gönderilen SYN paketlerinin algılanması ve alarm oluşturulması sağlanır. Güvenlik duvarı üzerinde yapılan kural tanımlamaları ile, hedef olarak belirlenen sisteme iletilecek maksimum paket sayısı için bir eşik değeri belirlenerek, sınırlandırma yapılabilir. Bu sınırlandırma ile, hedef sisteme gönderilmek istenen SYN paket sayısı, belirlenen eşik değerinden yüksek ise SYN flood tabanlı DoS/DDoS saldırısı olarak algılanır ve SYN paketlerinin düşürülmesi sağlanır.



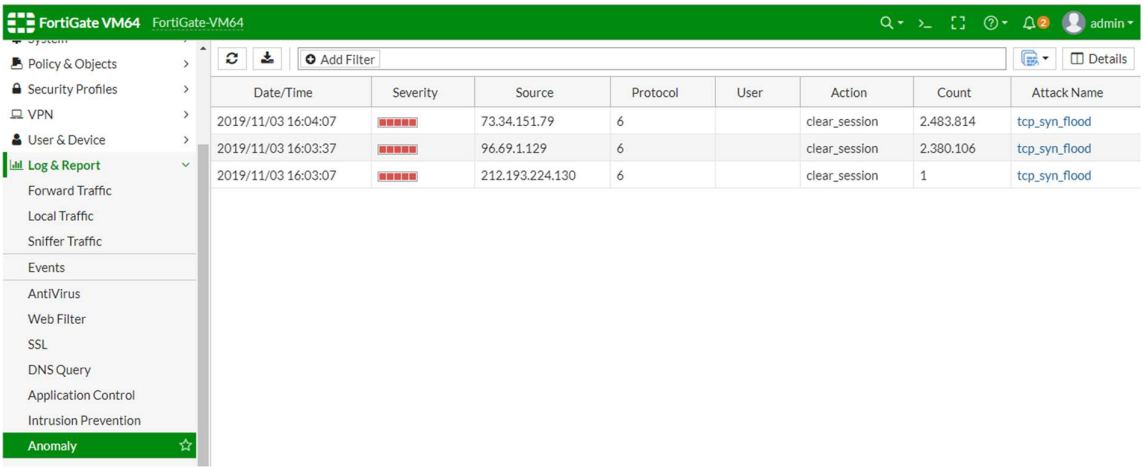
Şekil 3.20: Fortigate ile SYN flood tabanlı saldırılar için kural oluşturma.

Şekil 3.21'de, hedef sisteme gönderilmek istenen SYN paketlerinin ağ üzerinde oluşturduğu anomalinin tespit edildiği ve olası bir SYN flood tabanlı DoS/DDoS saldırısı yaşandığına dair alarm üretildiği gözlemlenmektedir. Saldırı sırasında alarm üretilmesine ek olarak, SIP-PBX sunucusu üzerinde ngrep, tcmdump, netstat gibi araçlar ile ağ trafiği izlenerek, saldırıların manuel olarak tespit edilmesi de sağlanabilir.



Şekil 3.21: Fortigate ile SYN flood saldırısı sırasında alarm üretme.

Gerçekleştirilen saldırı/saldırılar sırasında, saldırılara ilişkin tespit kayıtlarına Şekil 3.22'deki gibi Fortigate web arayüzü üzerinden erişilebilmektedir.



Şekil 3.22: Saldırı/saldırılar sırasında Fortigate'in saldırı tespit kayıtları.

4. BULGULAR

4.1.UDP VE SYN FLOOD TABANLI SALDIRI SONUÇLARININ ANALİZİ

Bu tez çalışmasında, hazırladığımız iki farklı laboratuvar ortamındaki çeşitli parametreler dikkate alınarak; "UDP Flood Tabanlı DoS", "UDP Flood Tabanlı DDoS", "SYN Flood Tabanlı DoS" ve "SYN Flood Tabanlı DDoS" saldırıları incelenmiştir. Bu saldırıların, hedef olarak belirlenen sistem üzerindeki etkileri ölçümlenmiş ve karşılaştırmalı olarak analiz edilmiştir.

Genel bir bakış açısı ile değerlendirdiğimizde; flood tabanlı DoS/DDoS saldırılarının sistem kaynaklarını tüketmeye yönelik saldırılar olduğu gözlemlenmiştir. Saldırı sırasında, hedef SIP sistemine kapasitesinden fazla sahte paket gönderilmesi; sistem üzerindeki işlem kapasitesinin artmasına neden olmaktadır. İşlem kapasitenin artması ile sistem üzerinde işlemci kullanım oranının da arttığı gözlemlenmiştir. Saldırganın, hedef sisteme ardışık olarak çok sayıda paket göndermesi; veri trafiğinde artış meydana getirir. Meydana gelen bu artış ile hedef sistemin yanıt sürelerinde gecikmeler yaşandığı gözlemlenmiştir.

Flood tabanlı saldırıların, sistem üzerindeki etkilerini en aza indirgemek ya da sistemin bu saldırılardan etkilenmemesini sağlamak amacıyla en temel güvenlik önlemlerinden biri olan güvenlik duvarları konumlandırılabilir. Güvenlik duvarı, üzerinden geçen trafiği filtreleme yeteneğine sahip olduğu için trafik akışını kontrol edebilmektedir. Güvenlik duvarı üzerinde yapılan kural tanımlamaları ile, üzerinden geçen trafiği sınırlandırabilmesi ve engelleyebilmesi sağlanmaktadır. Saldırı sırasında, saldırgan ya da saldırganlar tarafından gönderilen çok sayıda paketin hedef sisteme ulaşması engellenmiş ve veri trafiğinin stabil kalması sağlanmıştır.

Oluşturduğumuz saldırı senaryolarında; saniye bazında gönderilebilecek maksimum paket sayısı ile saldırıyı gerçekleştirecek makinenin/makinelerin kaynak gücü (işlemci, bellek) arasında doğru orantı ilişkisi kurulabilir. Saldırının gerçekleştireceği makinenin kaynak gücü ne kadar yüksek ise hedef sisteme saniyede gönderilecek paket sayısı da o kadar fazla olmaktadır. Bunun sonucunda hedef sistem kısa bir süre zarfında hizmet veremez hale gelmektedir.

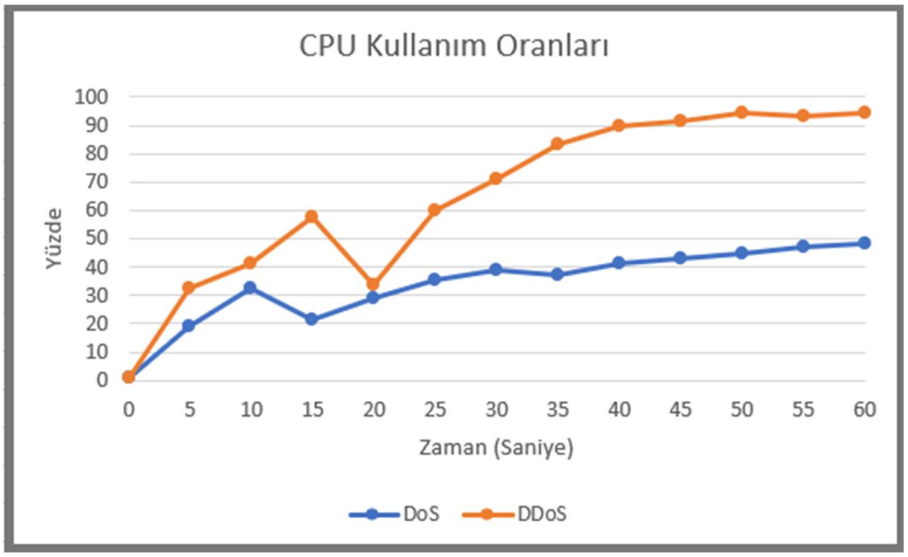
IPS/IDS gibi özellikleri içerisinde barındıran güvenlik duvarlarının yaklaşımlarını gözlemleyebilmek amacıyla tek bir kaynak ya da ağ üzerindeki birden fazla kaynak üzerinden

gönderilen sahte paketler ile iki farklı flood saldırısı, iki farklı senaryo ile gerçekleştirilmiş ve her bir senaryo için istatistikler toplanmıştır.

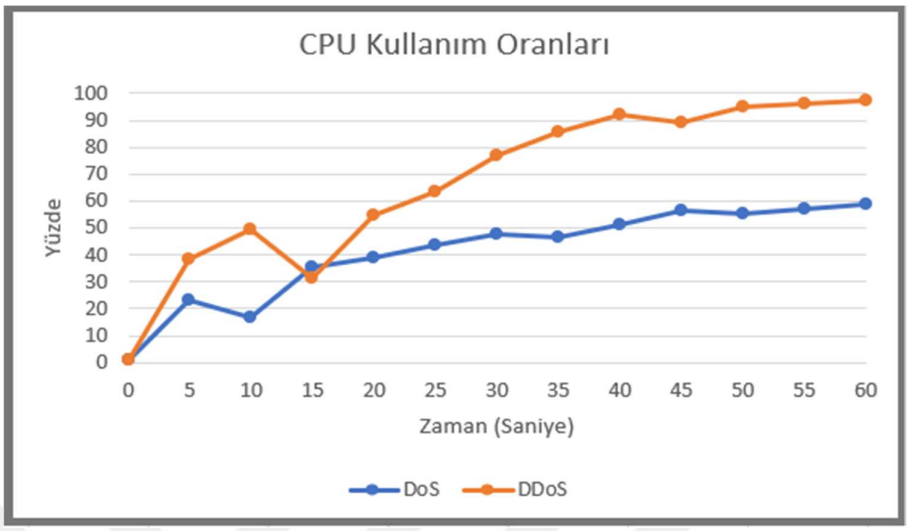
Hazırlanan saldırı senaryolarında, sahte IP adresi üretimi iki farklı şekilde gerçekleştirilmiştir. Üretilecek sahte IP adresi ya da IP adresleri manuel olarak belirlenebildiği gibi, istenilen sayı kadar random olarak da oluşturulabilmektedir. Güvenlik duvarlarının rate-limiting yöntemi ile IP adresi engelleme ve paket sayısı engelleme yaklaşımlarını inceleyebilmek amacıyla sahte IP adres üretimi gerçekleştirilmiştir.

Oluşturduğumuz iki farklı VoIP/SIP güvenlik laboratuvar ortamında, saldırı senaryoları gerçekleştirilirken 1 dakikalık, 3 dakikalık, 5 dakikalık ve 10 dakikalık süreler boyunca zamana göre işlemci kullanımını ve bellek kullanımını belirten istatistikler elde edilmiştir.

Elde edilen işlemci kullanım oranlarına ilişkin veriler, 1 dakikalık zaman dilimleri baz alınarak grafiksel olarak ifade edilmiştir. Flood tabanlı saldırılara maruz kalan savunmasız bir sistemin işlemci kullanım oranları Şekil 4.1 ve Şekil 4.2'de grafiksel şemalara dökülmüştür. Şekil 4.1'de UDP flood tabanlı saldırılara maruz kalan savunmasız bir sistemin 1 dakikalık süre boyunca CPU kullanım oranları gösterilir iken; Şekil 4.2'de SYN flood tabanlı saldırılar sırasında savunmasız bir sistemin CPU kullanım oranları gösterilmektedir. Gerçekleştirilen her bir saldırı senaryosunda, işlemci ve bellek tüketiminin zamana bağlı olarak arttığı gözlemlenmiştir.

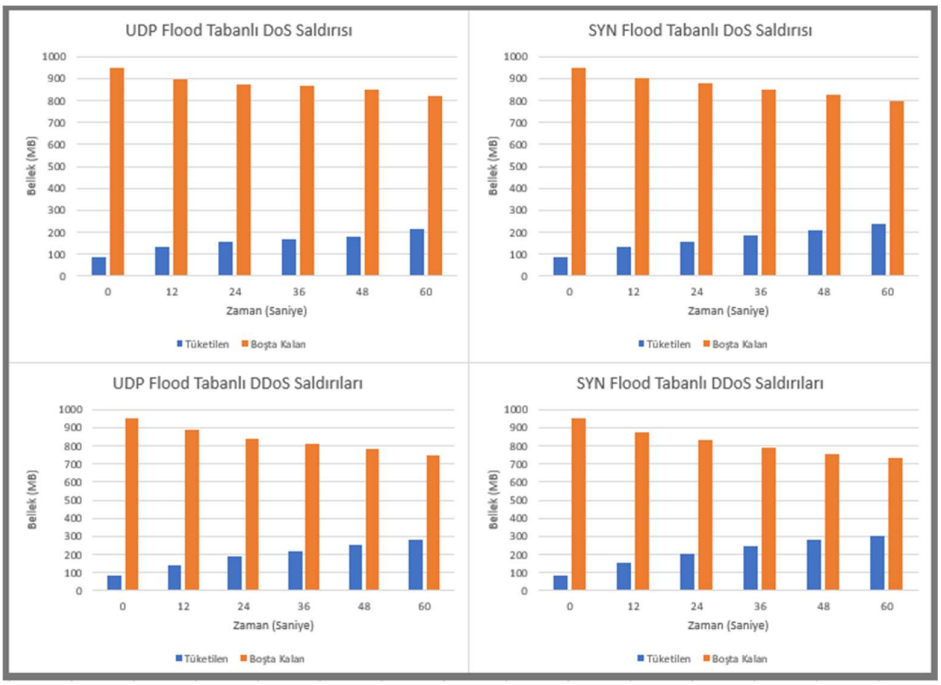


Şekil 4.1: Savunmasız bir sistemin UDP flood tabanlı saldırılar sırasında kullandığı CPU oranı.



Şekil 4.2: Savunmasız bir sistemin SYN flood tabanlı saldırılar sırasında kullandığı CPU oranı.

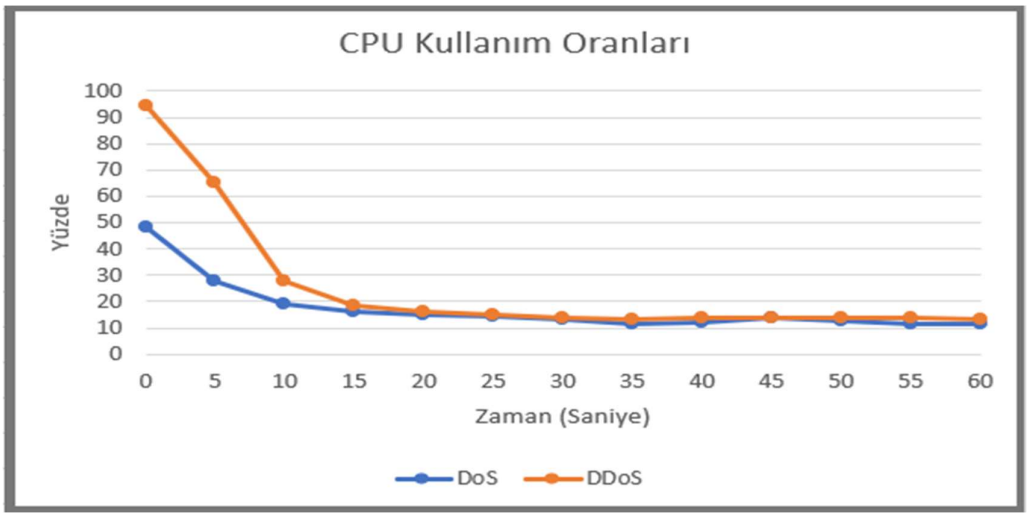
Savunmasız bir sistemi hedef alan flood tabanlı saldırılar sırasında bellek kullanımına ilişkin elde edilen veriler, 1 dakikalık zaman dilimleri baz alınarak Şekil 4.3'te grafiksel şemaya dökülmüştür. Saldırılar sırasında, kullanılan bellek miktarının zamana bağlı olarak arttığı gözlemlenmiştir.



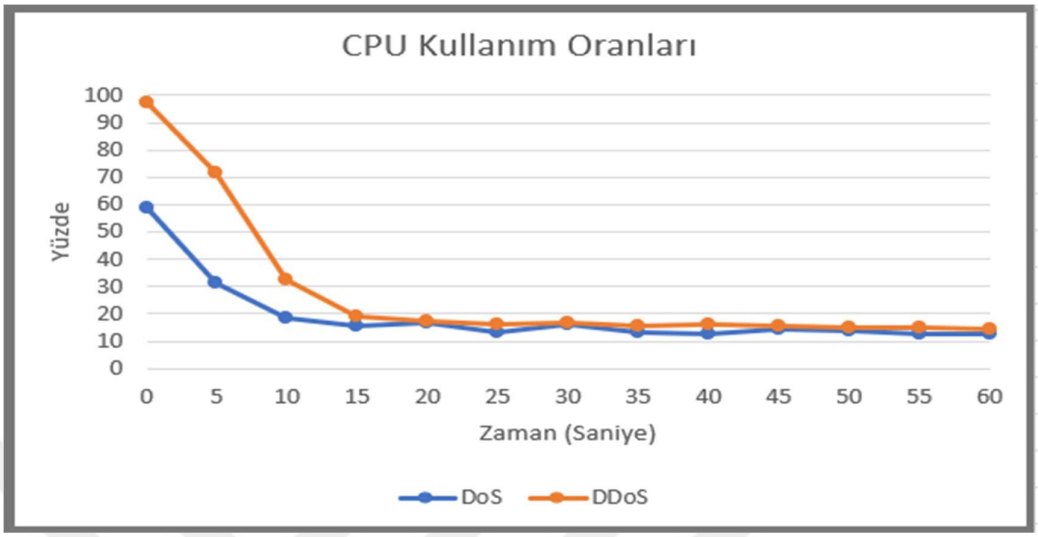
Şekil 4.3: Savunmasız bir sistemin flood tabanlı saldırılar sırasında harcadığı bellek miktarı.

Herhangi bir güvenlik mekanizması ile korunmayan bir sistemi hedef alan flood tabanlı saldırıları kendi aralarında karşılaştıracak olduğumuzda; ağ üzerinde birden fazla kaynak kullanılarak gerçekleştirilen DDoS saldırılarına maruz kalan bir sistemde tüketilen bellek oranı %8-%30 arasında değişmekte iken, tüketilen işlemci oranı %32-%97 arasında değişmektedir. Tek bir kaynak üzerinden gerçekleştirilen DoS saldırısında ise tüketilen bellek oranı %8-%23 arasında değişir iken; tüketilen işlemci oranı %19-%59 arasında değişmektedir. Elde edilen bu bilgiler doğrultusunda; DDoS saldırılarının DoS saldırısına kıyasla 1.47 kat daha etkili olduğu görülmüştür. Ek olarak savunmasız bir sistemi hedef alan UDP flood tabanlı ve SYN flood tabanlı saldırıları tüketilen kaynak bakımından ele aldığımızda; bu tarz saldırıların daha çok işlemci üzerinde etkili olduğu gözlemlenmiştir.

Güvenlik duvarı ile korunan bir sistemi hedef alan flood tabanlı saldırılar sırasında, elde edilen CPU kullanım oranlarına ilişkin veriler Şekil 4.4 ve Şekil 4.5'te grafiksel olarak ifade edilmiştir. UDP flood tabanlı saldırılar sırasında, güvenli bir sistemin 1 dakikalık zaman dilimi boyunca harcadığı CPU oranları Şekil 4.4'te gösterilmektedir. Şekil 4.5'te ise SYN flood tabanlı saldırılar sırasında, güvenli bir sistemin 1 dakikalık zaman dilimi boyunca harcadığı CPU değerleri gösterilmektedir. Güvenlik duvarı üzerinde kullanılan toplam paket sayısını sınırlandırma yaklaşımı ile flood tabanlı saldırılar sırasında, tüketilen CPU değerlerinin düştüğü gözlemlenmiştir.

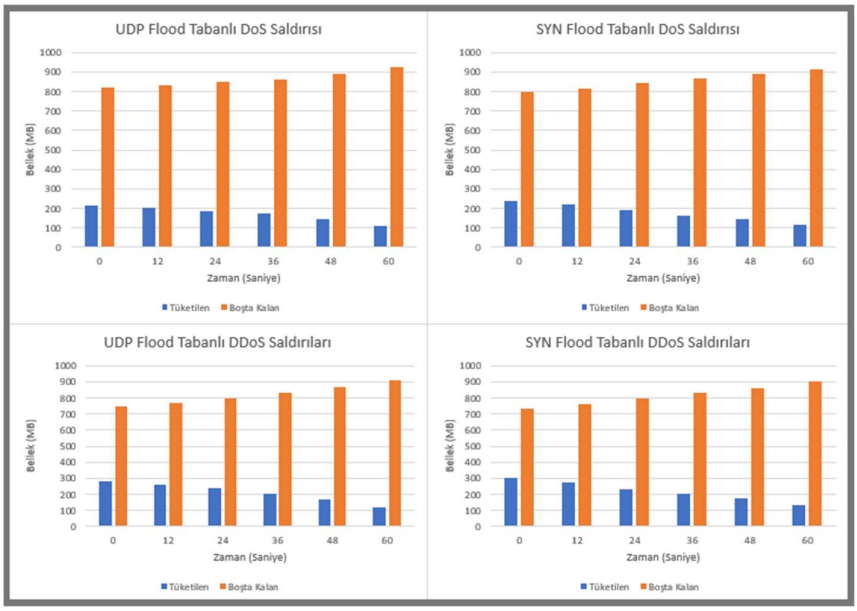


Şekil 4.4: Güvenli bir sistemin UDP flood tabanlı saldırılar sırasında kullandığı CPU oranı.



Şekil 4.5: Güvenli bir sistemin SYN flood tabanlı saldırılar sırasında kullandığı CPU oranı.

Güvenlik duvarı etkinleştirilmiş bir sistemi hedef alan UDP ve SYN flood tabanlı saldırılar sırasında, 1 dakikalık zaman dilimi boyunca tüketilen bellek miktarına ilişkin veriler Şekil 4.6'da grafiksel olarak ifade edilmiştir. Saldırılar sırasında, güvenlik duvarının etkinleştirilmesi ile hedef sistem tarafından kullanılan bellek miktarının zamana bağlı olarak azaldığı gözlemlenmiştir.



Şekil 4.6: Güvenli bir sistemin flood tabanlı saldırılar sırasında harcadığı bellek miktarı.

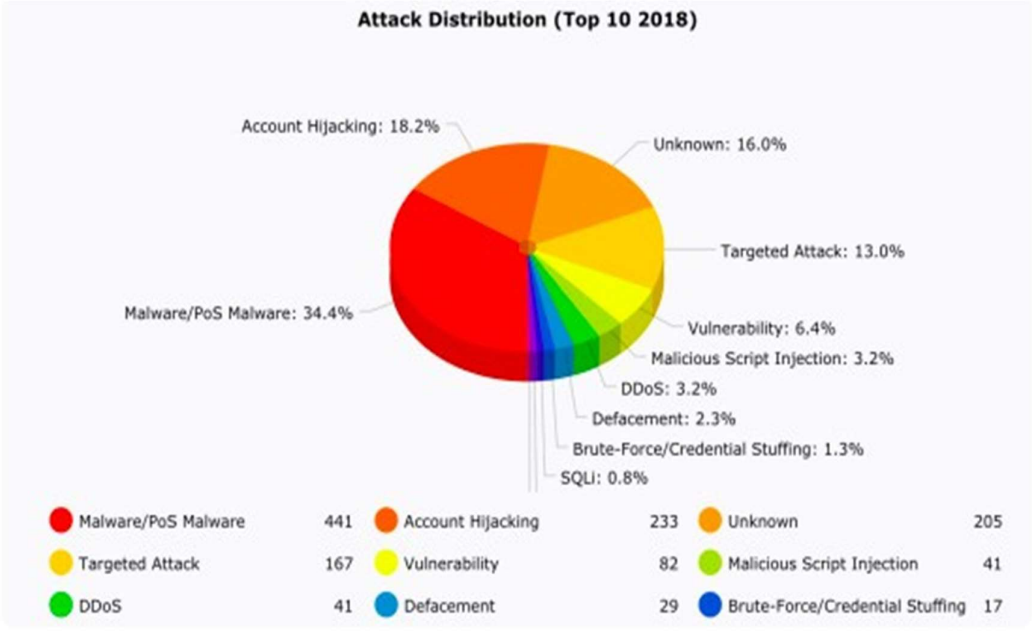
Güvenli bir sistemi hedef alan flood tabanlı saldırılar sırasında, saldırgan tarafından gönderilen paketler güvenlik duvarı tarafından karşılanmaktadır. Güvenlik duvarı üzerinde analiz edilen paket sayısı, eşik değerinden fazla olduğu için paketler engellenerek veri trafiğinin stabil kalması sağlanmaktadır. Hedef sistem üzerinde aşırı yüklenme gerçekleşmediği için tüketilen işlemci ve bellek oranı minimum düzeyde olduğu görülmektedir.

Saldırganlar tarafından hedef alınan sistemin anomali tespiti yapabilecek bir mekanizmaya sahip olması, saldırıların tespit edilmesini ve engellenmesini sağlamaktadır. Bu sayede yeni nesil telekom dünyasında yaşanabilecek flood tabanlı saldırılar karşısında orta ve büyük ölçekli şirketlerin, kurumsal firmaların, bankaların ve servis sağlayıcıların itibar kaybı ve gelir kaybı yaşamasının önüne geçilmesi sağlanacaktır.

5. TARTIŞMA VE SONUÇ

VoIP teknolojisi sağladığı düşük maliyet, kullanım kolaylığı ve hizmet kalitesi ile günümüzün popüler haberleşme teknolojilerinden biri haline gelmiştir. Ülkemizdeki ve dünyadaki popülerliğini her geçen gün arttıran VoIP teknolojisinin, SIP ile beraber kullanılmaya başlanması ile VoIP/SIP teknolojilerinin güvenlik zafiyetlerini hedef alan farklı özelliklerde birçok saldırı ile karşılaşılmaya başlanmıştır. Bu tez çalışması kapsamında incelenen flood tabanlı DoS ve DDoS saldırıları, IP protokolünün güvenlik açıklarının kullanılması ile hedef olarak belirlenen sistemin hizmet kalitesini düşürmeyi ve hizmet vermesini engellemeyi amaçlamaktadır.

VoIP/SIP sistemlerine yönelik gerçekleştirilen saldırılar arasında DoS ve DDoS saldırıları, en sık karşılaşılan ve en kolay gerçekleştirilen saldırı türleri arasında yer almaktadır. Bu saldırıları engelleyebilmek oldukça zor olduğu gibi hedef sistem üzerindeki etkileri de oldukça büyük olabilmektedir. Şekil 5.1'de, VoIP/SIP ağlarına yönelik saldırıları inceleyen 2018 yılına bir araştırmaya yer verilmiştir. Bu araştırmaya göre DDoS saldırılarının 2018 yılında en sık karşılaşılan saldırılar arasında yer aldığı gözlemlenmiştir [48].



Şekil 5.1: 2018 yılında VoIP/SIP sistemlerine yönelik gerçekleştirilen saldırılar ve dağılımları [48].

VoIP/SIP teknolojilerini hedef alan saldırıların birçoğu kritik seviyelerde gerçekleşmektedir ve özellikle son kullanıcıları, operatörleri ve servis sağlayıcıları olumsuz yönde etkilemektedir. Ülkemizde ve dünyada özellikle banka ve finans kuruluşlarını, operatörleri ve servis sağlayıcıları hedef alan kritik seviyede VoIP/SIP hacking olayları ile karşılaşılmaktadır. Ülkemizde yaşanan bu tip hacking olaylarına en yakın zamanlı örnek olarak, Ekim 2019 tarihinde gerçekleştirilen DDoS saldırıları verilebilir [49].

Bu tez çalışması kapsamında, VoIP/SIP teknolojilerinde sıkça karşılaşılan flood tabanlı DoS/DDoS saldırıları incelenmiş ve bu saldırıları önleyebilmek amacıyla güvenlik tavsiyeleri verilmiştir. Verilen güvenlik tavsiyeleri ile hedef sistem üzerinde yüksek seviyede bir ağ trafiğinin oluşması engellenmeye çalışılmış ve sistem kaynaklarının aşırı tüketilmesinin önüne geçilmesi hedeflenmiştir. Buna bağlı olarak flood tabanlı bir saldırı sırasında, siteme kayıtlı olan yasal kullanıcıların hizmet kalitesinde herhangi bir sapma yaşanmadan hizmet almaya devam etmeleri amaçlanmıştır.

VoIP/SIP teknolojilerini hedef alan çeşitli flood tabanlı DoS ve DDoS saldırı senaryoları bulunmaktadır. Aşağıda farklı saldırı senaryoları için farklı güvenlik tavsiyeleri verilmiştir.

Hedef alınan bir sisteme, tek bir saldırgan tarafından çok sayıda UDP ya da SYN paketleri gönderilerek DoS saldırısı gerçekleştirilebilir. Böyle bir durumda, hedef alınan sistemi dış saldırılardan korumak amacıyla güvenlik duvarları konumlandırılmalıdır. Güvenlik duvarı üzerinde bulunan rate-limiting özelliği kullanılarak, tek bir IP üzerinden ya da tek bir kaynak üzerinden gelecek paket sayısı sınırlandırılmalıdır.

Flood tabanlı saldırılarda; saldırgan IP Spoofing yöntemi ile tek bir kaynak üzerinden gönderilen UDP ya da SYN paketlerini, çok sayıda farklı kaynaktan geliyormuş gibi göstererek DDoS saldırıları gerçekleştirebilir. Böyle bir durumda, hedef sistemi dış saldırılardan korumak amacıyla güvenlik duvarları konumlandırılmalıdır. Güvenlik duvarı üzerinde bulunan rate-limiting özelliği ile, hedef sisteme iletilecek toplam paket sayısı sınırlandırılmalıdır.

Hedef alınan bir sisteme, tek bir saldırgan ya da birden çok saldırgan tarafından çok sayıda SYN paketi gönderilerek flood tabanlı saldırılar gerçekleştirilebilir. Böyle bir durumda, SYN Cookies özelliği olan bir güvenlik duvarı konumlandırılmalıdır. Hedef sistemin sahte IP adreslerinden gönderilen SYN paketleri için bellek tüketmesi engellenecektir. SYN Cookies özelliğinin aktif edilmesi ile hedef sistem kendisine ulaşan SYN paketleri için kaynak ayırmaz.

Hedef sistem, SYN paketine karşılık olarak göndereceği SYN-ACK paketi için özel bir ISN numarası hesaplanarak gönderilir. TCP üçlü el sıkışmasının son basamağı olan ACK paketi gönderildiğinde, ISN hesaplama işlemi tekrarlanır. ISN numaraları birbirleri ile eşleşmiyor ise bağlantı kurulmaz.

Yukarıda bahsedilen güvenlik tavsiyelerine ek olarak, VoIP/SIP sistemleri üzerinde yeterli düzeyde güvenlik bakış açısına sahip, nitelikli güvenlik uzmanları yetiştirilmelidir.

KAYNAKLAR

[1]. Netšajeva, S., 2013, *Penetration Testing Methodolgy for VoIP Call Center Provider,* Master's Thesis, Talinn University of Technology.

[2]. Davidson, J., Peters, J., Bhatia, M., Kalidindi, S., Mukherjee S., 2006, *Voice over IP Fundamentals: A systematic approach to understanding the basics of Voice over IP,* 2nd ed., Cisco Press, Inc., Indianapolis.

[3]. Çakır, C., 2009, *VoIP Teknolojilerinde Güvenlik,* Yüksek Lisans Tezi, T.C. Marmara Üniversitesi.

[4]. Sourabh, S., Arqum, H., Vibhakar, M., 2017, VoIP: Conceptual Model Implementation, *International Journal of Advanced Computational Engineering and Networking,* ISSN: 2320-2106, 51-54.

[5]. Information Sciences Institute University of Southern California 4676 Admiralty Way Marina del Rey, California, 1981, Internet Protocol, IETF RFC 791.

[6]. Information Sciences Institute University of Southern California 4676 Admiralty Way Marina del Rey, California, 1981, Transmission Control Protocol, IETF RFC 793.

[7]. Postel, J., 1980, User Datagram Protocol*,* IETF RFC 768.

[8]. Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V., 1996, RTP: A transport protocol for real-time applications, IETF 1889.

[9]. Schulzrinne, H., Frederick, R., Casner, S., Jacobson, V., 2003, RTP: A transport protocol for real-time applications, IETF RFC 3550.

[10]. Schulzrinne, H., Agboh, C., 2005, Session initiation protocol (SIP) - H.323 interworking requirements, IETF RFC 4123.

[11]. 2019, *Neden SIP, H.323 'den daha iyidir,* https://trueconf.com.tr/neden-sip-h-323-den-daha-iyidir/, [Ziyaret Tarihi: 10 Ekim 2019].

[12]. Andreasen, F., Foster, B., 2003*,* Media Gateway Control Protocol (MGCP) Version 1.0, IETF RFC 3435.

[13]. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E., 2002, SIP: Session initiation protocol, IETF RFC 3261.

[14]. Handley, M., Schulzrinne, H., Schooler, E., Rosenberg, J., 1999, SIP: Session initiation protocol, RFC 2543.

[15]. Radvision, SIP Protocol Overview, 2005, *VoIP developer solutions, video conference systems and infrastructures*.

[16]. Kaplan, Y., 2010, *SIP-(Session Initiation Protocol, Oturum Başlatma Protokolü),* https://www.yasinkaplan.com/tr/docs/SIP.pdf , [Ziyaret Tarihi: 10 Ekim 2019].

[17]. Kurt, B., Yıldız, Ç., Ceritli, T.Y., Cemgil, A.T., 2017, *A Bayesian change point model for detecting SIP-based DDoS Attacks, Digital Signal Processing.*

[18]. Handley, M., Jacobson, V., 1998., *SDP: session description protocol*, IETF RFC 2327.

[19]. Hagalisletto, A., M., Strand, L., 2010, Designing Attacks on SIP Call Setup, *International Journal of Applied Cryptography Volume 2 Issue 1,* 13-22.

[20]. Şahin, B., 2015, *DDoS Saldırılarına Karşı İstatistiksel Koruma Yaklaşımı*, Yüksek Lisans Tezi, T.C. Bahçeşehir Üniversitesi.

[21]. Flanagan, W. A., 2012, *VoIP and Unified Communications: Internet Telephony and the Future Voice network*, Hoboken, New Jersey: John Wiley and Sons, Inc.

[22]. Endler, D., & Collier, M., 2007. *Hacking exposed VoIP: voice over IP secrets and solutions*, McGraw-Hill/Osborne.

[23]. Akbar, A., Basha, M., Sattar *(IJIET)*, Volume 7 Issue August.

[24]. Walsh, T. J., Kuhn, D. R., Fries, S., 2005, *Security considerations for voice over IP systems*, Gaithersburg, MD: National Institute of Standards and Technology.

[25]. Sisalem, D., Floroiu, J., Kuthan, J., Abend, U., Schulzrinne, H., 2009, *SIP security*, NY: John Wiley and Sons, Ltd. Publication, New York.

[26]. Yüksel, M., 2017, *SIP (Session Initation Protocol) Saldırıları ve Önleme,* Yüksek Lisans, Gazi Üniversitesi Bilişim Enstitüsü.

[27]. Örencik, B., Yavaş, S., 2007, *VoIP Güvenliği*, https://slidex.tips/download/voip-gvenlii-a-gvenlii-prof-dr-blent-rencik-sinem-yava-bilgisayar-bilimleri, [Ziyaret Tarihi: 10 Ekim 2019].

[28]. Rosenberg, J., Jennings, C., 2008, The session initiation protocol (SIP) and spam, IETF RFC 5039.

[29]. Thermos, P., Takanen, A., 2007, *Securing VoIP networks, threats, vulnerabilities, and countermeasures*, Pearson Education, Boston.

[30]. Dwivedi, H., 2009, *Hacking VOIP: Protocols, Attacks, and Countermeasures*, No Starch Press, ISBN: 593271638.

[31]. Gençoğlu, H., 2017, *Hibrit Şifreleme Algoritması*, Doktora Tezi, T.C. Trakya Üniversitesi.

[32]. Şahin, F., 2015, Modern Blok Şifreleme Algoritmaları, *İstanbul Aydın Üniversitesi Dergisi 26,* 23-40.

[33]. Arslan, M., 2006, *Firewall*, Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü.

[34]. Kent, S., Atkinson, R., 1998, Security architecture for the internet protocol (IPSec), IETF RFC 2401.

[35]. Dierks, T., Allen, C., 1999, The TLS Protocol, IETF RFC 2246.

[36]. Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K., 2004, The Secure Real-time Transport Protocol (SRTP), RFC 3711.

[37]. 2007, *Oracle VM VirtualBox,* https://www.virtualbox.org/, [Ziyaret Tarihi: 10 Ekim 2019].

[38]. 1999, *Asterisk PBX,* https://www.asterisk.org/, [Ziyaret Tarihi: 10 Ekim 2019].

[39]. 2003, *Trixbox PBX,* https://www.voip-info.org/trixbox/, [Ziyaret Tarihi: 10 Ekim 2019].

[40]. 2015, *Kali Linux*, https://www.kali.org/, [Ziyaret Tarihi: 10 Ekim 2019].

[41]. 2006, *Wireshark,* https://www.wireshark.org/, [Ziyaret Tarihi: 10 Ekim 2019].

[42]. 2003, *Softphones*, https://www.zoiper.com/, [Ziyaret Tarihi: 10 Ekim 2019].

[43]. 2017, *Zenmap,* https://nmap.org/zenmap/, [Ziyaret Tarihi: 10 Ekim 2019].

[44]. 2006, *Network Grep Network Packet Analyzer,* http://ngrep.sourceforge.net, [Ziyaret Tarihi: 10 Ekim 2019].

[45]. 2014, *Htop Process Viewer*, http://hisham.hm/htop, [Ziyaret Tarihi: 10 Ekim 2019].

[46]. 1994, *Virtual Memory Statistics System Monitoring,* https://www.howtoforge.com/linux-vmstat-command/, [Ziyaret Tarihi: 10 Ekim 2019].

[47]. 2000, *Next Generation Firewall Fortigate,* https://www.fortinet.com/products/next-generation-firewall.html, [Ziyaret Tarihi: 10 Ekim 2019].

[48]. 2019, *2018 A Year of Cyber Attacks,* https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/, [Ziyaret Tarihi: 17 Kasım 2019].

[49]. 2019, *Türkiye'ye Siber Saldırı Şoku,* https://www.cybermagonline.com/turkiye039ye-siber-saldiri-soku-iki-buyuk-kurumdan-flas-aciklama-geldi, [Ziyaret Tarihi: 13 Kasım 2019].

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Kübra Sencar
Doğum Yeri	İstanbul
Doğum Tarihi	15.08.1991
Uyruğu	☑ T.C. ❒ Diğer:
Telefon	0536.652.25.57
E-Posta Adresi	sencarkubra@gmail.com
Web Adresi	-

Eğitim Bilgileri	
Lisans	
Üniversite	Trakya Üniversitesi
Fakülte	Mühendislik Fakültesi
Bölümü	Bilgisayar Mühendisliği Böümü
Mezuniyet Yılı	2014

Yüksek Lisans	
Üniversite	İstanbul Üniversitesi-Cerrahpaşa
Enstitü Adı	Lisansüstü Eğitim Enstitüsü
Anabilim Dalı	Bilgisayar Mühendisliği Anabilim Dalı
Programı	Bilgisayar Mühendisliği Programı

Makale ve Bildiriler
Sencar, K., Sakallı, T., Taş, M., 2014, "VoIP Güvenliği Kapsamında DoS Saldırılarının İncelenmesi, Örnek Senaryo Gerçekleştirme ve Güvenlik Politikası Geliştirme." *VII. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 17-18 Ekim 2014, İstanbul.