**GELİŞMİŞ GÜVENLİ DOSYA TRANSFER SİSTEMİ**

**Ağ Güvenliği ve Düşük Seviye Ağ Oluşturma Projesi Raporu**

**Merve Gök**

**GİRİŞ**

Gelişmiş Güvenli Dosya Transfer Sistemi, düşük seviye ağ protokolleri, güvenlik uygulamaları ve ağ performans analizi konularında uygulamalı deneyim sunan kapsamlı bir ağ oluşturma uygulamasıdır. Bu proje, IP paket manipülasyonu, kriptografik güvenlik önlemleri, ağ performans izleme ve saldırı simülasyon yetenekleri dahil olmak üzere modern ağ iletişiminin birden fazla kritik yönünü kapsamaktadır.

Sistem, hem pratik bir dosya transfer çözümü hem de ağ güvenliği açıklarını ve savunma programlama tekniklerini anlamak için eğitsel bir platform olarak hizmet vermektedir. Grafik kullanıcı arayüzü ile Python kullanılarak oluşturulan uygulama, güvenlik en iyi uygulamalarına odaklanırken ağ oluşturma kavramlarının gerçek zamanlı gösterimlerini sağlamaktadır.

Temel işlevsellik, AES-256 ve RSA şifreleme ile güvenli dosya transferi, manuel IP başlık oluşturma ve manipülasyonu, paket parçalanma işleme, ağ performans ölçüm araçları ve kapsamlı saldırı simülasyon modüllerini içermektedir. Bu çok yönlü yaklaşım, kullanıcıların hem teorik ağ oluşturma kavramlarını hem de gerçek dünya güvenlik uygulamalarını pratik olarak anlamalarını sağlar.

Proje, kimlik doğrulama mekanizmaları, SHA-256 hash'leme yoluyla bütünlük doğrulama ve şifreli iletişim kanalları uygulayarak çağdaş ağ güvenliği zorluklarını ele almaktadır. Ayrıca sistem, ortadaki adam saldırıları, paket enjeksiyonu ve trafik analizi senaryoları gibi yaygın ağ açıklarını göstererek saldırı simülasyon yetenekleri aracılığıyla eğitsel değer sağlamaktadır.

**TEKNİK DETAYLAR**

**Sistem Mimarisi**

Uygulama, beş temel bileşenden oluşan modüler bir mimari takip etmektedir: şifreleme işlemleri için CryptoManager, düşük seviye ağ işlevleri için NetworkUtils, performans metrikleri için NetworkAnalyzer, kullanıcı arayüzü yönetimi için SecureFileTransferGUI ve eğitsel amaçlar için çeşitli simülasyon modülleri.

Ana uygulama penceresi, beş farklı bölümden oluşan sekmeli arayüz tasarımını kullanmaktadır: Kimlik Doğrulama, Dosya Transferi, Güvenlik, Ağ Analizi ve Saldırı Simülasyonu. Her sekme, alttaki ağ oluşturma ve güvenlik sistemleriyle sorunsuz entegrasyon korurken özel işlevsellik sağlamaktadır.

**Düşük Seviye Ağ Oluşturma Uygulaması**

**IP Başlık Manipülasyonu**

NetworkUtils sınıfı, kapsamlı IP başlık oluşturma ve manipülasyon yetenekleri sağlamaktadır. create\_ip\_header() metodu, doğru sağlama toplamı hesaplamaları ile IPv4 başlıklarını manuel olarak oluşturarak IP protokol spesifikasyonlarının derin anlaşılmasını göstermektedir.

def create\_ip\_header(src\_ip, dst\_ip, payload\_len, ttl=64, flags=0):

version = 4

ihl = 5 # Internet Header Length

tos = 0 # Type of Service

tot\_len = 20 + payload\_len

identification = random.randint(1, 65535)

frag\_off = flags

protocol = 6 # TCP

Uygulama, ağ byte sırası (big-endian) kullanarak uygun byte sıralamasını içermekte ve standart IP sağlama toplamı algoritmasını uygulamaktadır. Sağlama toplamı hesaplaması RFC 791 spesifikasyonlarını takip ederek standart ağ oluşturma ekipmanları ile uyumluluğu sağlamaktadır.

**Paket Parçalanması**

Sistem, büyük veri yüklerini Maksimum İletim Birimi (MTU) kısıtlamalarına göre daha küçük parçalara bölen fragment\_data() metodu aracılığıyla manuel paket parçalanması uygular. Her parça, hedefteki doğru yeniden birleştirmeyi sağlayan uygun ofset bilgisi ve daha fazla parça bayrakları içermektedir.

Parçalanma algoritması, IP spesifikasyonlarının gerektirdiği şekilde parça sınırlarını 8-byte sınırlarında korur ve son parça hariç tüm parçalar için daha fazla parça bitini uygun şekilde ayarlar. Bu uygulama, gerçek ağlarda yönlendiricilerin paket parçalanmasını nasıl işlediğinin anlaşılmasını göstermektedir.

**Soket Programlama**

Uygulama, hem istemci hem de sunucu işlevselliği için ham soket programlama kullanmaktadır. Sunucu uygulaması, eşzamanlı bağlantıları işlemek için çoklu threading kullanırken, istemci uygulaması dosya transferleri sırasında sağlam hata işleme ve ilerleme raporlaması sağlamaktadır.

Soket seçenekleri, hızlı test döngüleri sırasında bağlama hatalarını önlemek için adres yeniden kullanımı (SO\_REUSEADDR) için yapılandırılmıştır. Uygulama, sistem kaynaklarının uygun şekilde yönetilmesini sağlamak için uygun soket temizleme ve istisna işleme içermektedir.

**Kriptografik Güvenlik Uygulaması**

**Şifreleme Sistemleri**

CryptoManager sınıfı, hem simetrik hem de asimetrik şifreleme algoritmalarını uygular. AES-256 şifreleme, her şifreleme işlemi için rastgele oluşturulan başlatma vektörleri ile Cipher Feedback (CFB) modunu kullanarak semantik güvenlik sağlamaktadır.

RSA-2048 şifreleme, SHA-256 hash'leme ile OAEP padding uygulayarak padding oracle saldırıları ve diğer kriptografik açıklara karşı koruma sağlamaktadır. Uygulama, güvenlik en iyi uygulamalarını korurken anahtar oluşturma, şifreleme ve şifre çözme işlemlerini uygun şekilde işlemektedir.

**Kimlik Doğrulama ve Bütünlük**

Kullanıcı kimlik doğrulaması, önceden tanımlanmış kullanıcı adı-şifre kombinasyonları ile kimlik bilgisi tabanlı bir sistem kullanmaktadır. Gösteri amaçları için basitleştirilmiş olsa da, kimlik doğrulama çerçevesi daha sağlam kimlik doğrulama mekanizmaları için temel sağlamaktadır.

Dosya bütünlük doğrulaması, transfer edilen dosyalar için benzersiz parmak izleri oluşturan SHA-256 kriptografik hash'leme kullanmaktadır. Sistem, şifrelemeden önce hash'leri hesaplar ve şifre çözmeden sonra bunları doğrulayarak transfer süreci boyunca veri bütünlüğünü sağlamaktadır.

**Anahtar Yönetimi**

Sistem, başlatma sırasında taze RSA anahtar çiftleri oluşturur ve AES anahtarlarını bellekte tutar. Gösteri amaçları için uygun olsa da, uygulama kriptografik olarak güvenli rastgele sayı üreteçleri kullanarak uygun anahtar oluşturmayı içermektedir.

**Ağ Performans Analizi**

**Gecikme Ölçümü**

NetworkAnalyzer sınıfı, yerel ping yardımcı programlarına sistem çağrıları kullanarak ping tabanlı gecikme ölçümü uygular. Uygulama, kapsamlı gecikme analizi sağlayarak minimum, maksimum ve ortalama yanıt sürelerini çıkarmak için ping çıktısını ayrıştırır.

Gecikme ölçüm işlevi, Windows ve Unix benzeri sistemler için uygun ping komut parametrelerini kullanarak farklı işletim sistemlerine uyum sağlar. Sonuçlar, ping çıktısından zamanlama bilgilerini çıkarmak için düzenli ifadeler kullanılarak ayrıştırılır.

**Bant Genişliği ve Paket Kaybı Simülasyonu**

Gerçek bant genişliği testi iperf gibi özel araçlar gerektirse de, sistem ağ performans ölçümünde yer alan kavramları gösteren simülasyon yetenekleri sağlamaktadır. Simülasyon, çeşitli bağlantı türleri için beklenen aralıklarda gerçekçi değerler üretir.

Paket kaybı simülasyonu, paket kaybının ağ performansını ve güvenilirliğini nasıl etkilediğini göstererek eğitsel değer sağlamaktadır. Simülasyon, gerçekçi kayıp yüzdeleri üretir ve paket iletim başarı oranlarının istatistiksel analizini sağlar.

**Saldırı Simülasyonu ve Güvenlik Farkındalığı**

**Ortadaki Adam (MITM) Saldırı Simülasyonu**

MITM simülasyonu, saldırganların güvenli olmayan iletişimlerde ağ trafiğini nasıl yakalayıp değiştirebileceğini göstermektedir. Simülasyon, paket yakalama, veri değiştirme ve bu tür saldırıları önlemede şifrelemenin önemini göstermektedir.

Uygulama, gerçekçi paket akış senaryoları oluşturur ve saldırganların transit halindeki verileri nasıl değiştirebileceğini gösterir. Bu eğitsel bileşen, modern ağ oluşturmada uçtan uca şifrelemenin kritik önemini vurgulamaktadır.

**Paket Enjeksiyon Simülasyonu**

Paket enjeksiyon simülasyonu, saldırganların ağ akışlarına kötü amaçlı paketleri nasıl ekleyebileceğini göstermektedir. Scapy mevcut olduğunda, simülasyon uygun başlık ve yüklerle gerçek paket yapıları oluşturur.

Simülasyon, keyfi kaynak adresleri ve yük verileri ile sahte paketlerin nasıl oluşturulabileceğini göstererek enjeksiyon saldırılarını önlemede paket kimlik doğrulama ve güvenli protokollerin önemini göstermektedir.

**Trafik Analizi Gösterimi**

Trafik analizi modülü, saldırganların şifrelenmemiş ağ trafiğinden nasıl bilgi edinebileceğini simüle eder. Simülasyon, şifreli ve şifrelenmemiş iletişimler arasındaki farkı göstererek hassas bilgilerin düz metin protokollerinden nasıl çıkarılabileceğini göstermektedir.

**Grafik Kullanıcı Arayüzü Uygulaması**

GUI, profesyonel görünüm ve sezgisel kullanıcı deneyimi sağlamak için temalı widget'lar (ttk) ile Tkinter kullanmaktadır. Sekmeli arayüz tasarımı, mantıksal iş akışı ilerlemesini korurken farklı işlevsel alanları ayırmaktadır.

İlerleme çubukları dosya transferleri sırasında görsel geri bildirim sağlarken, kaydırmalı metin widget'ları tüm sistem işlemleri için kapsamlı günlük bilgilerini görüntüler. Arayüz tasarımı, gelişmiş ağ özelliklerine erişim sağlarken netlik ve kullanım kolaylığını öncelendirir.

**Hata İşleme ve Sağlamlık**

Uygulama, tüm ana bileşenler boyunca kapsamlı hata işleme içermektedir. Soket işlemleri, timeout işleme ve zarif bağlantı sonlandırma içerir. Kriptografik işlemler, hatalı veri ve anahtar hataları için uygun istisna işleme içerir.

Dosya işlemleri, dosya varlığı, izinler ve disk alanı kullanılabilirliği kontrollerini içerir. Ağ işlemleri, bağlantı arızaları, timeout'lar ve protokol hataları için işleme içerir.

**KISITLAMALAR VE İYİLEŞTİRMELER**

**Mevcut Kısıtlamalar**

**Kriptografik Uygulama Kısıtlamaları**

Mevcut RSA uygulaması, RSA şifrelemesinin matematiksel kısıtlamaları nedeniyle küçük dosya boyutları ile sınırlıdır. Yaklaşık 190 byte'tan büyük dosyalar RSA-2048 ile doğrudan şifrelenemez, pratik kullanım için hibrit şifreleme yaklaşımları gerektirir.

AES anahtar yönetim sistemi şu anda kalıcı anahtar depolama veya anahtar değişim mekanizmaları olmadan her oturum için yeni anahtarlar üretmektedir. Üretim ortamlarında, çok kullanıcılı senaryolar için güvenli anahtar değişim protokolleri gerekli olacaktır.

Kimlik doğrulama sistemi, şifre hash'leme veya tuzlama mekanizmaları olmadan statik kimlik bilgisi depolaması kullanmaktadır. Modern kimlik doğrulama sistemleri, bcrypt veya Argon2 gibi algoritmalar kullanarak güvenli şifre depolaması gerektirecektir.

**Ağ Uygulama Kısıtlamaları**

Ham soket uygulaması, çoğu işletim sisteminde yönetici ayrıcalıkları gerektirerek dağıtım esnekliğini sınırlamaktadır. Kullanıcı-alanı ağ oluşturma veya konteyner teknolojileri kullanan alternatif yaklaşımlar bu sınırlamayı ele alabilir.

IP başlık oluşturma işlevi şu anda yalnızca IPv4 protokollerini desteklemektedir. Modern ağ uygulamaları, çağdaş ağ altyapıları ile uyumluluğu sağlamak için IPv6 desteği içermelidir.

Paket parçalanma uygulaması, çekirdek ağ yığınları ile etkileşim olmadan kullanıcı alanında çalışmaktadır. Gerçek dünya uygulamaları, çekirdek seviyesi parçalanma ve yeniden birleştirme mekanizmalarını dikkate almalıdır.

**Performans ve Ölçeklenebilirlik Kısıtlamaları**

Mevcut sunucu uygulaması, yüksek eşzamanlılık senaryoları için verimli ölçeklenmeyebilecek bağlantı başına thread modeli kullanmaktadır. Asenkron G/Ç veya olay güdümlü mimariler daha iyi ölçeklenebilirlik özellikleri sağlayacaktır.

Ağ performans ölçüm araçları, yerel ölçüm algoritmaları uygulamak yerine harici yardımcı programlara dayanmaktadır. Bu bağımlılık, taşınabilirlik ve ölçüm parametreleri üzerindeki kontrolü sınırlamaktadır.

Bant genişliği test yeteneği, gerçek verim ölçümü uygulamak yerine şu anda simüle edilmektedir. Gerçek bant genişliği testi, koordineli istemci-sunucu ölçüm protokolleri gerektirecektir.

**Planlanan İyileştirmeler**

**Gelişmiş Kriptografik Özellikler**

Anahtar değişimi için RSA'yı toplu veri şifrelemesi için AES ile birleştiren hibrit şifreleme uygulaması, güvenliği korurken dosya boyutu sınırlamalarını ele alacaktır. Bu yaklaşım, keyfi büyük dosyaların güvenli transferini sağlayacaktır.

RSA veya ECDSA kullanarak dijital imza yeteneklerinin eklenmesi, inkar edilemezlik ve kimlik doğrulama doğrulaması sağlayacaktır. Dijital imzalar, gönderen özgünlüğü ve mesaj bütünlüğünü aynı anda sağlayacaktır.

Diffie-Hellman veya ECDH gibi güvenli anahtar değişim protokollerinin uygulanması, dinamik anahtar oluşturma ve güvenli çok taraflı iletişim senaryolarını sağlayacaktır.

**Gelişmiş Ağ Özellikleri**

IPv6 destek uygulaması, modern ağ altyapıları ile uyumluluğu sağlayacak ve uygulamayı geleceğe hazırlayacaktır. Bu, IPv6 başlık oluşturma, adresleme ve ikili yığın işlem yeteneklerini içermektedir.

Hizmet Kalitesi (QoS) özelliklerinin uygulanması, farklı trafik türlerinin önceliklendirilmesini ve bant genişliği tahsis yönetimini sağlayacaktır. Bu, özellikle kurumsal dağıtım senaryolarında değerli olacaktır.

Ağ Adres Çevirisi (NAT) geçiş yeteneklerinin eklenmesi, uçtan uca bağlantının doğrudan mevcut olmadığı tipik ağ ortamlarında bağlantıyı iyileştirecektir.

**Kullanıcı Deneyimi İyileştirmeleri**

Sürükle ve bırak dosya seçimi uygulaması, kullanıcı arayüzü sezgiliğini ve iş akışı verimliliğini iyileştirecektir. Bu, yaygın işlemler için gereken tıklama sayısını azaltacaktır.

Dosya transfer devam ettirme yeteneklerinin eklenmesi, güvenilmez ağ bağlantıları üzerinden büyük dosya transferleri için güvenilirliği iyileştirecektir. Bu, kontrol noktası oluşturma ve kısmi transfer kurtarma mekanizmalarını içerecektir.

Toplu dosya transfer yeteneklerinin uygulanması, tek kimlik doğrulama ve kurulum prosedürleri ile birden fazla dosyanın verimli transferini sağlayacaktır.

**Güvenlik ve İzleme İyileştirmeleri**

Paket yakalama ve analizi ile gerçek zamanlı ağ izleme yetenekleri, ağ davranışı ve güvenlik olayları hakkında daha derin içgörüler sağlayacaktır. Bu, protokol analizi ve anomali tespit özelliklerini içerecektir.

İzinsiz giriş tespit yeteneklerinin uygulanması, şüpheli ağ etkinlikleri veya saldırı kalıpları için gerçek zamanlı güvenlik izleme ve uyarı oluşturma sağlayacaktır.

Kurcalamaya dayanıklı günlük depolama ile denetim günlüğünün eklenmesi, güvenlik olayı araştırması için hesap verebilirlik ve adli tıp yetenekleri sağlayacaktır.

**Uygulanan Bonus Özellikler**

**Kapsamlı Saldırı Simülasyon Çerçevesi**

Uygulama, temel gereksinimlerin ötesinde giden kapsamlı bir saldırı simülasyon çerçevesi içermektedir. Bu, ağ güvenliği tehditlerini anlamak için eğitsel değer sağlayan MITM saldırı simülasyonu, paket enjeksiyon gösterimleri ve trafik analizi yeteneklerini içermektedir.

**Gelişmiş Kriptografik Algoritma Desteği**

Sistem, farklı güvenlik senaryoları için kullanıcılara seçenekler sağlayan hem AES-256 hem de RSA-2048 dahil olmak üzere birden fazla şifreleme algoritması uygular. Uygulama, uygun padding şemaları ve güvenli rastgele sayı üretimi içermektedir.

**Ağ Performans Analiz Araçları**

Gecikme analizi, bant genişliği test simülasyonu ve paket kaybı ölçümü dahil olmak üzere ağ performans ölçüm araçlarının entegrasyonu, temel dosya transfer işlevselliğinin ötesinde kapsamlı ağ analizi yetenekleri sağlamaktadır.

**Profesyonel GUI Uygulaması**

Kapsamlı günlükleme, ilerleme gösterimi ve sezgisel iş akışı tasarımı ile çok sekmeli grafik arayüz, temel komut satırı arayüzü gereksinimlerini aşar ve profesyonel düzeyde kullanıcı deneyimi sağlar.

**SONUÇ**

Gelişmiş Güvenli Dosya Transfer Sistemi, düşük seviye ağ kavramları, güvenlik uygulamaları ve ağ performans analizinin kapsamlı anlaşılmasını başarıyla göstermektedir. Proje, IP başlık manipülasyonu, soket programlama, kriptografik güvenlik önlemleri ve saldırı simülasyon yeteneklerinin pratik uygulaması yoluyla tüm belirtilen öğrenme çıktılarını başarır.

Düşük seviye ağ oluşturma ile uygulamalı deneyim, manuel IP başlık oluşturma, paket parçalanma algoritmaları ve ham soket programlama yoluyla gösterilmektedir. Uygulama, ağ protokolleri ve bunların gerçek dünya senaryolarındaki pratik uygulamalarının derin anlaşılmasını göstermektedir.

Ağ performans metriklerinin pratik anlaşılması, gecikme ölçüm araçları, bant genişliği analiz yetenekleri ve paket kaybı simülasyonu uygulaması yoluyla başarılmaktadır. Bu özellikler, ağ sorun giderme ve optimizasyon için gerekli nicel analiz yetenekleri sağlamaktadır.

Güvenlik risklerine ve savunma programlamaya maruz kalma, MITM saldırıları, paket enjeksiyon senaryoları ve trafik analizi tekniklerini gösteren saldırı simülasyon çerçevesi aracılığıyla kapsamlı olarak ele alınmaktadır. Savunma uygulamaları, şifreleme, kimlik doğrulama ve bütünlük doğrulama mekanizmalarını içermektedir.

Proje, hem işlevsel bir dosya transfer sistemi hem de ağ güvenliği kavramlarını anlamak için eğitsel bir platform olarak hizmet vermektedir. Kapsamlı günlükleme, kullanıcı dostu arayüz ve ayrıntılı dokümantasyon, onu hem pratik kullanım hem de eğitsel amaçlar için uygun hale getirmektedir.

Modüler mimari ve kapsamlı hata işleme, ağ oluşturma ve güvenlik kavramlarına odaklanmayı korurken yazılım mühendisliği en iyi uygulamalarını göstermektedir. Uygulama, üretim ortamlarında güvenlik ve güvenilirlik standartlarını korurken bu iyileştirmeler için sağlam bir temel sağlamaktadır.

Gelecekteki geliştirme fırsatları arasında gelişmiş kriptografik özellikler, IPv6 desteği, iyileştirilmiş ölçeklenebilirlik ve ek güvenlik izleme yetenekleri bulunmaktadır. Mevcut uygulama, güvenlik ve güvenilirlik standartlarını korurken bu iyileştirmeler için sağlam bir temel sağlamaktadır.

Proje, teorik ağ kavramları ile pratik uygulama arasındaki boşluğu başarıyla kapatarak düşük seviye ağ oluşturma, güvenlik programlama ve ağ performans analizi ile değerli uygulamalı deneyim sağlamaktadır. Kapsamlı özellik seti ve profesyonel uygulama, belirtilen öğrenme çıktılarının ustalığını göstermekte ve gelişmiş ağ oluşturma ve güvenlik uygulamaları için temel sağlamaktadır.

**KAYNAKLAR**

Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8. baskı). Pearson.

Stallings, W. (2020). *Network security essentials: Applications and standards* (6. baskı). Pearson.

Python Software Foundation. (2024). Python 3.12 dokümantasyonu - Soket programlama. https://docs.python.org/3/library/socket.html adresinden alınmıştır.

Cryptography.io. (2024). Cryptography dokümantasyonu - Fernet simetrik şifreleme. https://cryptography.io/en/latest/ adresinden alınmıştır.

Internet Engineering Task Force. (1981). *Internet Protocol - DARPA Internet Program Protocol Specification* (RFC 791). https://tools.ietf.org/rfc/rfc791.txt adresinden alınmıştır.

Internet Engineering Task Force. (1981). *Transmission Control Protocol - DARPA Internet Program Protocol Specification* (RFC 793). https://tools.ietf.org/rfc/rfc793.txt adresinden alınmıştır.

National Institute of Standards and Technology. (2001). *Advanced Encryption Standard (AES)* (FIPS PUB 197). U.S. Department of Commerce.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.

Scapy Community. (2024). Scapy dokümantasyonu - Paket manipülasyon programı. https://scapy.readthedocs.io/ adresinden alınmıştır.

Tkinter Documentation. (2024). Python GUI programming with Tkinter. https://docs.python.org/3/library/tkinter.html adresinden alınmıştır.

**Kodlar için Github Linki:** [**https://github.com/merveegokk/g-venli-dosya-transferi**](https://github.com/merveegokk/g-venli-dosya-transferi)

**Youtube Video Linki:** <https://youtu.be/Um8sDUMjiqA>