Ağ Güvenliği Kavramları - Özet Doküman

Hazırlayan: Furkan Yaşar *LinkedIn*

Bu doküman, temel seviyede Ağ Güvenliği Kavramları ilgili özet bilgiler içerir.

1 Siber Güvenliğin Mevcut Durumu

ÖNEMLİ: Siber suçlular artık kritik altyapıları ve sistemleri çökertmek için gerekli uzmanlığa ve araçlara sahiptir.

Güvenlik Terimleri

Terim	Açıklama
Varlık (Asset)	Organizasyon için değerli olan her şey (insanlar, ekipmanlar, kaynaklar, veri)
Zafiyet (Vulnerability)	Bir tehdit tarafından istismar edilebilecek sistem veya tasarım zayıflığı
Tehdit (Threat)	Şirket varlıkları, verileri veya ağ işlevselliği için potansiyel tehlike
İstismar (Exploit)	Bir zafiyetten yararlanma mekanizması
Azaltma (Mitigation)	Potansiyel tehdit veya riskin olasılığını veya şiddetini azaltan karşı önlem
Risk	Bir tehdidin, bir organizasyonu olumsuz etkileme amacıyla bir varlığın zafiyetinden yararlanma olasılığı

Ağ Saldırı Vektörleri

- Saldırı vektörü: Bir tehdit aktörünün sunucu, ana bilgisayar veya ağa erişim sağlayabileceği yol
- İç tehditler, dış tehditlerden daha büyük hasara neden olma potansiyeline sahiptir

Veri Kaybı

- Veri kaybı veya veri sızıntısı: Verilerin kasıtlı veya kazara kaybolması, çalınması veya dış dünyaya sızdırılması
- Veri kaybı sonuçları:
    - Marka hasarı ve itibar kaybı
    - Rekabet avantajı kaybı
    - Müşteri kaybı
    - Gelir kaybı
    - Dava/hukuki işlemler ve para cezaları

Veri Kaybı Vektörleri

Vektör	Açıklama
E-posta/Sosyal Ağlar	Ele geçirilen e-posta veya anlık mesajlar gizli bilgileri açığa çıkarabilir
Şifrelenmemiş Cihazlar	Veri şifrelenmemişse, hırsız değerli gizli verileri alabilir
Bulut Depolama Cihazları	Zayıf güvenlik ayarları nedeniyle buluta erişim tehlikeye girerse hassas veriler kaybolabilir
Çıkarılabilir Medya	Yetkisiz veri transferi veya kayıp USB sürücüleri
Basılı Kopyalar	Gizli veriler artık gerekli değilse parçalanmalıdır
Uygunsuz Erişim Kontrolü	Ele geçirilen zayıf parolalar tehdit aktörlerine kolay erişim sağlar

2 Tehdit Aktörleri

Hacker Türleri

Tür	Açıklama
Beyaz Şapkalı Hacker	Etik hacker'lar, programlama becerilerini iyi, etik ve yasal amaçlarla kullanır
Gri Şapkalı Hacker	Kişisel kazanç veya hasar vermek için olmasa da suç işleyen ve tartışmalı etik dışı şeyler yapan bireyler
Kara Şapkalı Hacker	Kişisel kazanç veya kötü niyetli nedenlerle bilgisayar ve ağ güvenliğini ihlal eden etik dışı suçlular

Modern Hacking Terimleri

Terim	Açıklama
Script Kiddies	Mevcut komut dosyalarını, araçları ve istismarları çalıştıran gençler veya deneyimsiz hacker'lar
Zafiyet Aracısı (Vulnerability Broker)	Genellikle gri şapkalı hacker'lar, istismarları keşfedip satıcılara rapor eder
Hacktivist	Kuruluşları veya hükümetleri kamuoyu önünde protesto eden gri şapkalı hacker'lar
Siber Suçlular	Serbest çalışan veya büyük siber suç örgütleri için çalışan kara şapkalı hacker'lar
Devlet Destekli	Hükümet sırlarını çalan, istihbarat toplayan ve ağları sabote eden beyaz veya kara şapkalı hacker'lar

Siber Suçlular

- Siber suçluların tüketicilerden ve işletmelerden milyarlarca dolar çaldığı tahmin ediliyor
- Yeraltı ekonomisinde çalışırlar, saldırı araç setlerini, sıfır gün istismar kodlarını, botnet hizmetlerini satın alır ve satarlar

Hacktivistler

- Anonymous ve Suriye Elektronik Ordusu gibi gruplar
- Nispeten temel, ücretsiz araçlara güvenirler

Devlet Destekli Hacker'lar

- Gelişmiş, özelleştirilmiş saldırı kodu oluştururlar
- Daha önce keşfedilmemiş yazılım zafiyetlerini (sıfır gün) kullanırlar
- Örnek: İran'ın nükleer zenginleştirme yeteneklerine zarar vermek için oluşturulan Stuxnet kötü amaçlı yazılımı

3 Tehdit Aktörü Araçları

Sızma Testi Araçları

Araç Türü	Açıklama	Örnekler
Parola Kırıcılar	Parolaları kırmak veya kurtarmak için kullanılır	John the Ripper, Ophcrack, L0phtCrack
Kablosuz Hacking Araçları	Kablosuz ağlara sızmak için kullanılır	Aircrack-ng, Kismet, InSSIDer
Ağ Tarama ve Hacking Araçları	Ağ cihazlarını, sunucuları ve ana bilgisayarları taramak için	Nmap, SuperScan, Angry IP Scanner
Paket Oluşturma Araçları	Güvenlik duvarlarını test etmek için özel olarak hazırlanmış sahte paketler kullanır	Hping, Scapy, Yersinia
Paket Dinleyicileri	Geleneksel Ethernet LAN'larında veya WLAN'larda paketleri yakalar ve analiz eder	Wireshark, Tcpdump, Ettercap
Rootkit Dedektörleri	Yüklü rootkit'leri tespit etmek için kullanılır	AIDE, Netfilter, PF: OpenBSD
Zafiyet Tarayıcılar	Ağ veya sistemde açık portları belirlemek için	Nessus, OpenVAS, SAINT

Saldırı Türleri

Saldırı Türü	Açıklama
Dinleme Saldırısı	Tehdit aktörünün ağ trafiğini yakaladığı ve "dinlediği" saldırı
Veri Değiştirme Saldırısı	Tehdit aktörlerinin şirket trafiğini ele geçirmesi ve paketteki verileri değiştirmesi
IP Adresi Sahteciliği	Tehdit aktörünün, kurumsal intranet içindeki geçerli bir adresten geliyormuş gibi görünen bir IP paketi oluşturması
Parola Tabanlı Saldırılar	Tehdit aktörleri geçerli bir kullanıcı hesabı keşfederse, gerçek kullanıcı ile aynı haklara sahip olurlar
Hizmet Reddi (DoS) Saldırısı	Bir DoS saldırısı, geçerli kullanıcıların bir bilgisayarın veya ağın normal kullanımını engeller
Ortadaki Adam (MitM) Saldırısı	Tehdit aktörlerinin kendilerini bir kaynak ile hedef arasına yerleştirdiği saldırı

4 Kötü Amaçlı Yazılım (Malware)

Virüsler ve Truva Atları

- Virüsler yayılmak ve diğer bilgisayarlara bulaşmak için insan eylemi gerektirir
- Virüsler bilgisayar koduna, yazılıma veya belgelere kendini ekleyerek gizlenir

Virüs Türleri

Tür	Açıklama
Boot Sektör Virüsü	Önyükleme sektörüne, dosya bölümleme tablosuna veya dosya sistemine saldırır
Firmware Virüsleri	Cihaz firmware'ine saldırır
Makro Virüsü	MS Office makro özelliğini kötüye kullanır
Program Virüsleri	Kendisini başka bir çalıştırılabilir programa ekler

Truva Atı Türleri

Tür	Açıklama
Uzaktan Erişim	Yetkisiz uzaktan erişim sağlar
Veri Gönderen	Tehdit aktörüne parolalar gibi hassas veriler sağlar
Yıkıcı	Dosyaları bozar veya siler
Proxy	Kurbanın bilgisayarını saldırı başlatmak için kaynak cihaz olarak kullanır

Diğer Kötü Amaçlı Yazılım Türleri

Tür	Açıklama
Adware	İstenmeyen reklamlar gösterir, genellikle çevrimiçi yazılım indirilerek dağıtılır
Fidye Yazılımı (Ransomware)	Kullanıcının dosyalarına erişimini engeller, şifreler ve şifre çözme anahtarı için fidye talep eder
Rootkit	Tehdit aktörlerinin bir bilgisayara yönetici hesap düzeyinde erişim kazanması için kullanılır
Casus Yazılım (Spyware)	Kullanıcı hakkında bilgi toplar ve kullanıcının rızası olmadan tehdit aktörlerine gönderir
Solucan (Worm)	Kullanıcı eylemleri olmadan yasal yazılımdaki zafiyetlerden yararlanarak otomatik olarak yayılan kendi kendini kopyalayan program

5 Yaygın Ağ Saldırıları

Keşif (Reconnaissance) Saldırıları

- Tehdit aktörleri, yetkisiz keşif ve sistem, hizmet veya zafiyetlerin haritalanması için keşif saldırılarını kullanır
- Teknikler:
    - Hedef hakkında bilgi sorgulama
    - Hedef ağda ping taraması başlatma
    - Aktif IP adreslerinde port taraması başlatma
    - Zafiyet tarayıcıları çalıştırma
    - Sömürü araçlarını çalıştırma

Erişim Saldırıları

- Kimlik doğrulama hizmetlerinde, FTP hizmetlerinde ve web hizmetlerinde bilinen zafiyetlerden yararlanır
- Türler:
    - Parola Saldırıları
    - Spoofing Saldırıları (IP spoofing, MAC spoofing, DHCP spoofing)
    - Güven İstismarı
    - Port Yönlendirmeleri
    - Ortadaki Adam Saldırıları
    - Arabellek Taşması Saldırıları

Sosyal Mühendislik Saldırıları

Saldırı Türü	Açıklama
Pretexting (Bahane Üretme)	Tehdit aktörü, alıcının kimliğini doğrulamak için kişisel veya finansal verilere ihtiyacı olduğunu iddia eder
Phishing (Oltalama)	Tehdit aktörü, alıcıyı cihazına kötü amaçlı yazılım yüklemeye veya kişisel/finansal bilgileri paylaşmaya ikna etmek için meşru, güvenilir bir kaynaktan geliyormuş gibi görünen sahte e-posta gönderir
Spear Phishing (Hedefli Oltalama)	Tehdit aktörü, belirli bir birey veya kuruluş için özel olarak hazırlanmış hedefli bir oltalama saldırısı oluşturur
Spam	Genellikle zararlı bağlantılar, kötü amaçlı yazılım veya aldatıcı içerik içeren istenmeyen e-posta
Quid pro quo (Bir Şey için Bir Şey)	Tehdit aktörünün bir taraftan hediye karşılığında kişisel bilgi istemesi

DoS ve DDoS Saldırıları

- Hizmet Reddi (DoS) saldırısı, kullanıcılara, cihazlara veya uygulamalara ağ hizmetlerinde bir tür kesinti oluşturur
- İki ana DoS saldırısı türü:
    - **Çok Fazla Trafik** - Tehdit aktörü, ağın, ana bilgisayarın veya uygulamanın kaldıramayacağı bir hızda muazzam miktarda veri gönderir
    - **Kötü Niyetle Biçimlendirilmiş Paketler** - Tehdit aktörü, bir ana bilgisayara veya uygulamaya kötü niyetle biçimlendirilmiş bir paket gönderir ve alıcı bunu işleyemez
- Dağıtılmış DoS Saldırısı (DDoS), DoS saldırısına benzer, ancak birden çok koordineli kaynaktan kaynaklanır

6 IP Zafiyetleri ve Tehditler

IPv4 ve IPv6

- IP, bir pakette bulunan kaynak IP adresinin gerçekten o kaynaktan gelip gelmediğini doğrulamaz
- Tehdit aktörleri sahte kaynak IP adresi kullanarak paket gönderebilir

IP İlişkili Saldırılar

Saldırı Türü	Açıklama
ICMP Saldırıları	Tehdit aktörleri, Internet Control Message Protocol (ICMP) yankı paketlerini (ping) korumalı bir ağdaki alt ağları ve ana bilgisayarları keşfetmek, DoS sel saldırıları oluşturmak ve ana bilgisayar yönlendirme tablolarını değiştirmek için kullanır
Amplifikasyon ve Yansıtma Saldırıları	Tehdit aktörleri, meşru kullanıcıların bilgilere veya hizmetlere erişmesini engellemek için DoS ve DDoS saldırılarını kullanır
Adres Sahteciliği Saldırıları	Tehdit aktörleri, gönderenin kimliğini gizlemek veya başka bir meşru kullanıcı gibi davranmak için sahte kaynak IP adresi bilgisine sahip paketler oluşturur
Ortadaki Adam Saldırısı (MITM)	Tehdit aktörleri kendilerini bir kaynak ile hedef arasına yerleştirerek iletişimi şeffaf bir şekilde izler, yakalar ve kontrol eder
Oturum Ele Geçirme	Tehdit aktörleri fiziksel ağa erişim sağlar ve ardından bir oturumu ele geçirmek için bir MITM saldırısı kullanır

ICMP Saldırıları

- Tehdit aktörleri, keşif ve tarama saldırıları için ICMP kullanır
- ICMP mesajları:
    - ICMP echo request ve echo reply
    - ICMP unreachable
    - ICMP mask reply
    - ICMP redirects
    - ICMP router discovery

7 TCP ve UDP Zafiyetleri

TCP Segment Başlığı

- TCP segment bilgileri IP başlığından hemen sonra görünür
- TCP segmentinin altı kontrol biti:
    - **URG** - Acil işaretçi alanı anlamlı
    - **ACK** - Onay alanı anlamlı
    - **PSH** - İtme fonksiyonu
    - **RST** - Bağlantıyı sıfırla
    - **SYN** - Sıra numaralarını senkronize et
    - **FIN** - Göndericiden daha fazla veri yok

TCP Hizmetleri

- **Güvenilir Teslimat** - TCP, teslimatı garanti etmek için onayları içerir
- **Akış Kontrolü** - TCP bu sorunu ele almak için akış kontrolünü uygular
- **Durum Bilgili İletişim** - İki taraf arasındaki TCP stateful iletişimi TCP üç yönlü el sıkışması sırasında gerçekleşir

TCP Saldırıları

- **TCP SYN Flood Saldırısı**:
    1. Tehdit aktörü bir web sunucusuna birden çok SYN isteği gönderir
    2. Web sunucusu her SYN isteği için SYN-ACK'lar ile yanıt verir ve üç yönlü el sıkışmasını tamamlamak için bekler
    3. Geçerli bir kullanıcı web sunucusuna erişemez çünkü web sunucusunda çok fazla yarı açık TCP bağlantısı vardır
- **TCP Reset Saldırısı**: Tehdit aktörü, bir veya her iki uç noktaya TCP RST içeren sahte bir paket gönderir
- **TCP Oturum Ele Geçirme**: Tehdit aktörü, hedefle iletişim kurarken zaten kimliği doğrulanmış bir ana bilgisayarı devralır

UDP Segment Başlığı ve İşlemi

- UDP genellikle DNS, TFTP, NFS ve SNMP tarafından kullanılır
- Bağlantısız bir taşıma katmanı protokolüdür
- TCP'den çok daha düşük ek yüke sahiptir

UDP Saldırıları

- UDP herhangi bir şifreleme ile korunmaz

- **UDP Flood Saldırıları**: Tehdit aktörü, genellikle sahte bir ana bilgisayardan, alt ağdaki bir sunucuya bir UDP paketi seli göndermek için UDP Unicorn veya Low Orbit Ion Cannon gibi bir araç kullanır

8 IP Hizmetleri

ARP Zafiyetleri

- Ana bilgisayarlar, belirli bir IP adresine sahip bir ana bilgisayarın MAC adresini belirlemek için segmentteki diğer ana bilgisayarlara bir ARP İsteği yayınlar
- Herhangi bir istemci, "gratuitous ARP" adı verilen istenmeyen bir ARP Yanıtı gönderebilir
- Bir tehdit aktörü, trafiği yeniden yönlendirmek için MITM saldırısı oluşturmak amacıyla yerel ağdaki cihazların ARP önbelleğini zehirleyebilir

DNS Saldırıları

- **DNS Açık Çözümleyici Saldırıları**:
  - DNS önbellek zehirlenmesi saldırıları
  - DNS amplifikasyon ve yansıtma saldırıları
  - DNS kaynak kullanımı saldırıları
- **DNS Gizli Saldırıları**:
  - Fast Flux (Hızlı Akış)
  - Double IP Flux (Çift IP Akışı)
  - Domain Generation Algorithms (Alan Adı Üretme Algoritmaları)
- **DNS Alan Gölgeleme Saldırıları**: Tehdit aktörü, saldırılar sırasında kullanılmak üzere sessizce birden çok alt etki alanı oluşturmak için etki alanı hesabı kimlik bilgilerini toplar
- **DNS Tünelleme**: Tehdit aktörleri, DNS trafiği içine DNS olmayan trafik yerleştirir

DHCP Saldırıları

- **DHCP Sahteciliği Saldırısı**: Sahte bir DHCP sunucusu ağa bağlandığında ve meşru istemcilere yanlış IP yapılandırma parametreleri sağladığında meydana gelir
- Sahte sunucu çeşitli yanıltıcı bilgiler sağlayabilir:
  - Yanlış varsayılan ağ geçidi
  - Yanlış DNS sunucusu
  - Geçersiz IP adresi

9 Ağ Güvenliği En İyi Uygulamaları

Gizlilik, Kullanılabilirlik ve Bütünlük (CIA)

- **Gizlilik (Confidentiality)** - Yalnızca yetkili kişiler, varlıklar veya süreçler hassas bilgilere erişebilir
- **Bütünlük (Integrity)** - Verilerin yetkisiz değişiklikten korunması
- **Kullanılabilirlik (Availability)** - Yetkili kullanıcıların önemli kaynaklara ve verilere kesintisiz erişimi olmalıdır

Derinlemesine Savunma Yaklaşımı

- Hem genel hem de özel ağlar arasında güvenli iletişim sağlamak için yönlendiriciler, anahtarlar, sunucular ve ana bilgisayarlar dahil cihazların güvenliğini sağlamalısınız
- Uygulanan güvenlik cihazları ve hizmetleri:
  - VPN
  - ASA Güvenlik Duvarı
  - IPS (Saldırı Önleme Sistemi)
  - ESA/WSA (E-posta/Web Güvenliği Cihazları)
  - AAA Sunucusu (Kimlik Doğrulama, Yetkilendirme, Hesap Yönetimi)

Güvenlik Duvarı (Firewall)

- Ağlar arasında erişim kontrol politikasını uygulayan bir sistem veya sistem grubudur
- Politikalar:
  - Herhangi bir harici adresten web sunucusuna gelen trafiğe izin ver
  - FTP sunucusuna giden trafiğe izin ver
  - İç IMAP sunucusuna gelen trafiği reddet
  - Tüm gelen ICMP echo isteği trafiğini reddet

Saldırı Önleme Sistemi (IPS)

- Hızlı hareket eden ve gelişen saldırılara karşı savunmak için, ağın giriş ve çıkış noktalarına entegre edilmiş uygun maliyetli algılama ve önleme sistemlerine ihtiyacınız olabilir
- IDS ve IPS teknolojileri algılayıcı olarak dağıtılır
- İmzalar kullanılarak ağ trafiğindeki kalıpları tespit eder

İçerik Güvenliği Cihazları

- **Cisco E-posta Güvenliği Cihazı (ESA)**: Simple Mail Transfer Protocol'ü (SMTP) izlemek için tasarlanmış özel bir cihaz
- **Cisco Web Güvenliği Cihazı (WSA)**: Web tabanlı tehditler için azaltma teknolojisi

10 Kriptografi

Güvenli İletişimin Dört Unsuru

- **Veri Bütünlüğü** - Mesajın değiştirilmediğini garanti eder
- **Köken Kimlik Doğrulaması** - Mesajın sahte olmadığını ve belirtilen kişiden geldiğini garanti eder
- **Veri Gizliliği** - Yalnızca yetkili kullanıcıların mesajı okuyabileceğini garanti eder
- **Veri İnkar Edilemezliği** - Göndericinin gönderilen bir mesajın geçerliliğini inkar edemeyeceğini garanti eder

Hash Fonksiyonları

Fonksiyon	Anahtar Uzunluğu	Durum
MD5	128-bit	Eski algoritma, mümkünse SHA-2 kullanılmalı
SHA-1	160-bit	Bilinen kusurları var, mümkünse SHA-2 kullanılmalı
SHA-2	224-512-bit	Yeni nesil algoritma, mümkün olduğunda kullanılmalı

Simetrik Şifreleme

- Verileri şifrelemek ve şifresini çözmek için aynı önceden paylaşılmış anahtar kullanılır
- VPN trafiği gibi büyük miktarda veriyi şifrelemek için yaygın olarak kullanılır
- Algoritmalar:
    - DES (Data Encryption Standard)
    - 3DES (Triple DES)
    - AES (Advanced Encryption Standard)
    - SEAL (Software-Optimized Encryption Algorithm)
    - RC4 (Rivest Cipher 4)

Asimetrik Şifreleme

- Şifreleme için kullanılan anahtar, şifre çözme için kullanılan anahtardan farklıdır
- Bir genel anahtar ve bir özel anahtar kullanır
- Algoritmalar:
    - Diffie-Hellman (DH)
    - DSS/DSA (Digital Signature Standard/Algorithm)
    - RSA (Rivest, Shamir, Adleman)
    - ElGamal
    - Elliptical Curve (Eliptik Eğri)

Diffie-Hellman Anahtar Anlaşması

- İki bilgisayarın daha önce iletişim kurmadan özdeş paylaşılan bir gizli anahtar oluşturduğu asimetrik bir matematiksel algoritmadır
- Yeni paylaşılan anahtar aslında gönderici ve alıcı arasında hiçbir zaman değiş tokuş edilmez
- Kullanım örnekleri:
    - IPsec VPN kullanılarak veri değişimi
    - İnternet üzerinden SSL veya TLS kullanılarak veri şifreleme
    - SSH veri değişimi