BMÜ-457 AĞ GÜVENLİĞİ

10.hafta Özet ders slaytları

2020-21- Güz Dönemi

Görevler ve Tanımlamalar

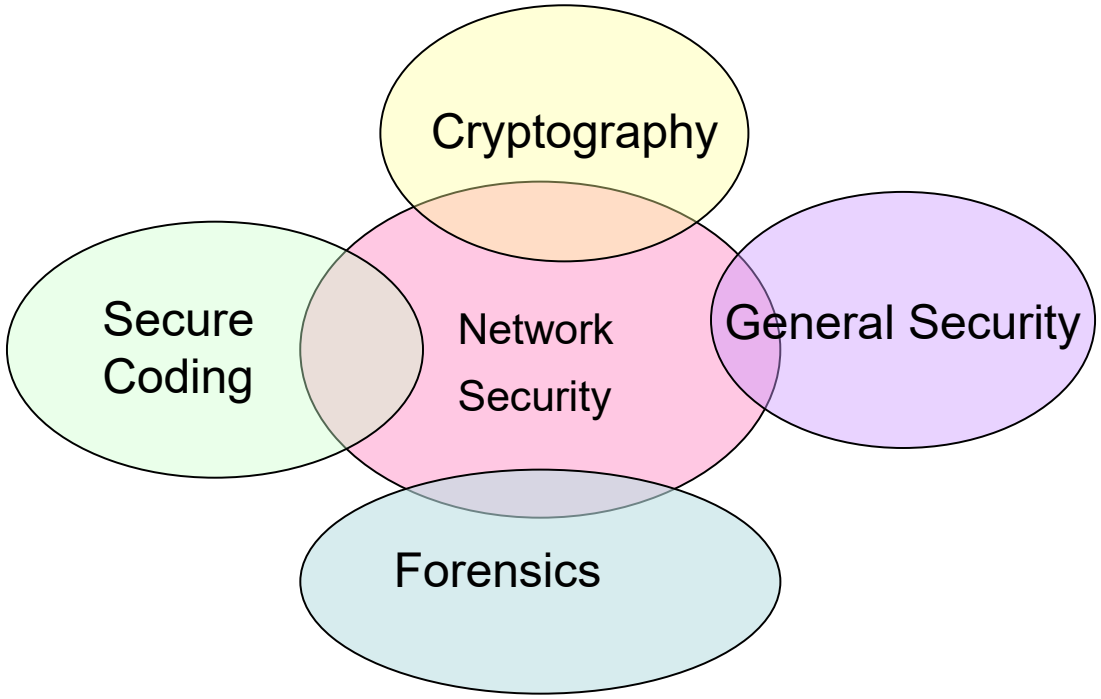
Bir sayısal cihazda hafızalanmış olan veya işlenen veya bir ağda seyahat eden veriler için;

- ***Confidentiality (Gizlilik)***
- ***İntegrity (Bütünlük)***
- ***Non-repudiation (İnkar edememe)***
- ***Availability (Kullanılabilirlik- Bilginin her ihtiyaç duyulduğunda yetkili kişlerce erişilebilir ve kullanılabilir olmasıdır)***

özelliklerinin garanti edilmiş, yani güvenliğinin sağlanmış olması gerekir.

Ağ Güvenliği = Bilgisayar Güvenlik sistemi + İletişim Güvenliği

- Ağ güvenliği; ağa bağlı bilgisayar sistemlerini ve ağdaki bilgisayarlarda saklanan veya ağ üzerinde iletilen verileri korumak içindir. Not:İnternet(public network)'in kullandığı IPV.4 TCP/IP protokolu güvensiz bir protokol topluluğudur. Niye?



Ağ Güvenliği

- Ağ güvenliği çözümlerini;

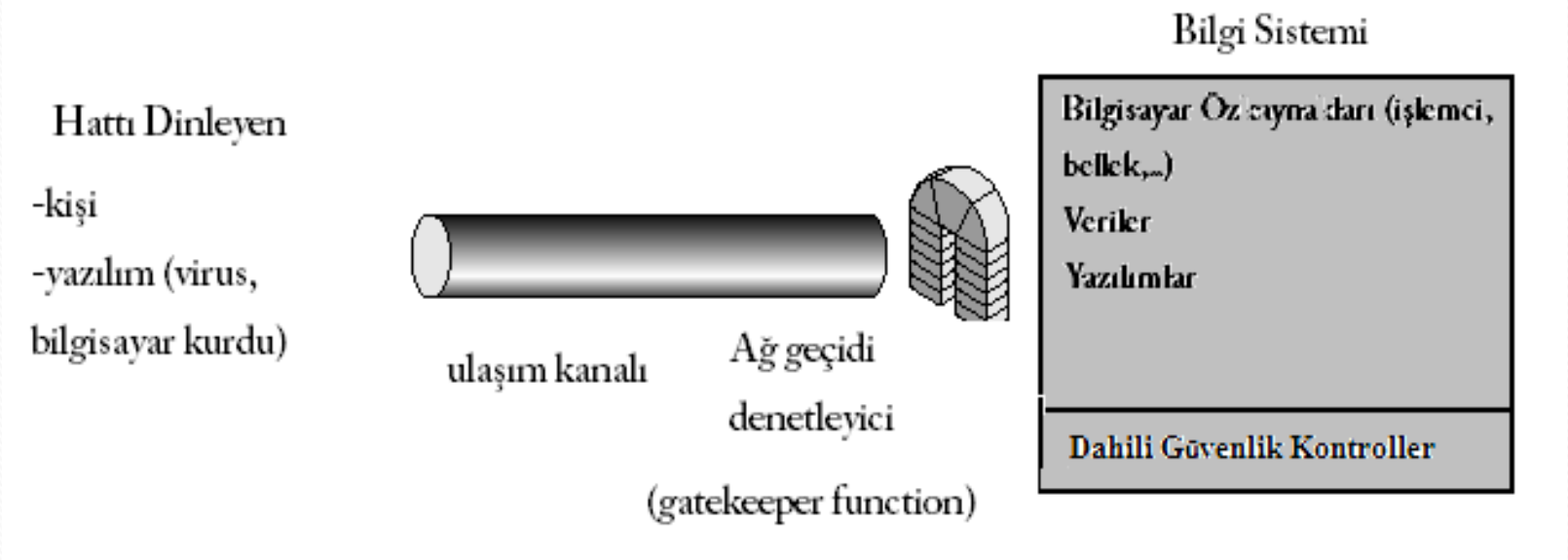
  - Kriptografik

  -Sistem tabanlı (Erişim Güvenliği temelli)

  çözümler olarak ikiye ayırmak mümkündür.

- Sistem tabanlı çözümler kriptografik işlemler içermeyen, sistem bilgilerini kullanarak güvenliği sağlamaya çalışan çözümlerdir.
- Örnek olarak yerel ağı dışarıdan gelecek saldırılardan korumayı amaçlayan güvenlik duvarları ve olası başarılı saldırıları anlamaya yönelik sızma denetim (IDS) sistemleri verilebilir.

Ağ Erisim Güvenlik Modeli (Sistem Tabanlı Cözüme Örnek)



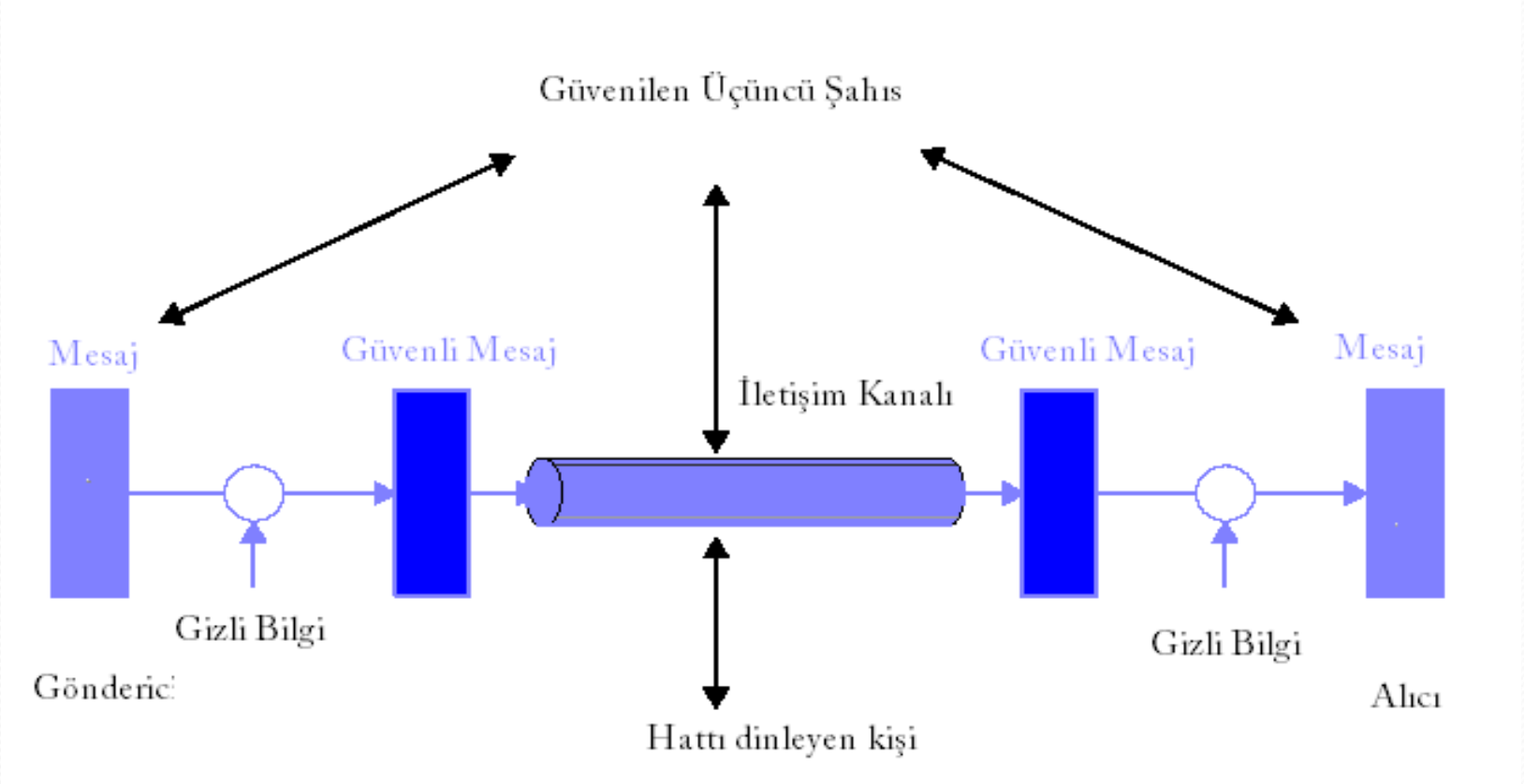
Bilgi sistemlerine (ağlara, Bilgisayarlara, Server'lara v.b) istenmeyen erişimin engellenmesi işlemidir.

Bu modeli için:

Kullanıcıları tanıyan uygun bir ağ geçidi denetleyici seçmek (pasword temelli erişim, erişim yetkisi ve seviyesi belirleme)

- Dahili Güvenlik Kontrolü uygulaması (Sistemi devamlı izleyerek anormal olayları sezmek ve tehditleri önceden belirleyebilmek- STS v.b)

Bir Ağ Güvenliği Modeli (Kriptografik tabanlı Güvenlik)



Gönderici ve alıcı mesajları belirli şifreleme algoritmalarına göre gizli olarak üretilip, iletirken, güvenli bir üçüncü şahıs gizli bilgilerin dağıtıcısı olarak hizmet vermekte, her iki taraf arasında noter görevi görmektedir. Bunlara sertifika otoriteleri denir.

OSI Güvenlik Mimarisi X.800

- Veri güvenliğinde sistematik bir yaklaşım olarak; ITU-T (İnternational Telecomunication Union - Telecommunication Standardization Sector) kuruluşunun X.800 olarak adlandırdığı standartlara uyulur.

- X.800 Aynı zamanda yedi katmanlı OSI Temel Referans Modelinde güvenlik hizmetlerinin uygulanması içinde uygundur.

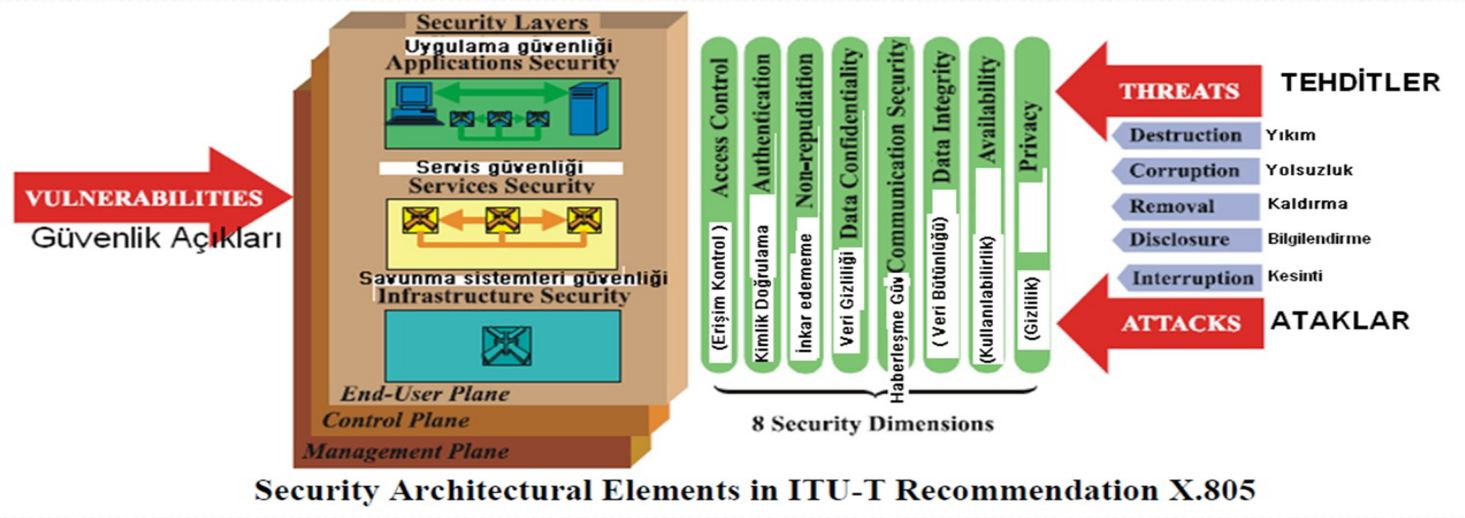
Güvenlik mimarisi uçtan uca güvenlikle ilgili üç ana soruyu ele alır;

1) Ne tür bir korumaya ihtiyaç duyuluyor ve hangi tehditlere karşı gerekli?

2) Korunması gereken farklı ağ teçhizatı türleri ve tesis grupları nelerdir?

3) Korunması gereken farklı ağ faaliyetleri türleri nelerdir?

- Bu sorular ***güvenlik boyutları (security dimensions), güvenlik katmanları (security layers) ve güvenlik düzlemleri (security planes)*** olmak üzere üç mimari bileşen tarafından ele alınmaktadır.
- Güvenlik mimarisi tarafından açıklanan ilkeler, ağın teknolojisi veya protokol yığını içindeki konumundan bağımsız olarak çok çeşitli ağlara uygulanabilir.



Security Architectural Elements in ITU-T Recommendation X.805

8 adet Güvenlik Boyutu, Ağın güvenlik açıklarının bütününü kapsar. 8 adet Güvenlik boyutunun herbiri ağ saldırılarının belirli bir kısmının önlenmesi için gereken önlemleri açıklar.

Sekiz güvenlik boyutu, herbir güvenlik perspektifine (Katmanlar ve planlara) uygulanır.

- Ağ elemanlarına, servislere, uygulamalara erişimin limitlenmesi ve kontrolu. Yetkisiz erişimleri önlemek için.

Örnek:password, ACL, firewall

Access Control (Erişim Kontrolu)

Authentication (Kimlik Doğrulama)

İletişim kuracak varlıkların biribirlerinin kimliklerini doğrulamaları içindir.

Örnek: Paylaşılan gizli kod dizisi, PKI, digital imza, digital sertifika.

- Ağda oluşan tüm aktivitelerin inkar edilememesinin sağlanması.

Örnek: sistem log'ları, digital imzalar.

Non-repudiation (İnkar edememe)

Data Confidentiality (Veri gizliliği)

Verilerin gizliliğinin sağlanması. Veri içeriğinin yetkisiz kişiler tarafından anlaşılmamasını sağlar.Örn:Kriptolama

- Verilerin, sadece kaynaktan hedefe aktığından emin olunması.
- Örnek.: VPN, MPLS, L2TP

Communication Security (İletişim Gizliliği)

Data Integrity (Veri Bütünlüğü)

- Datanın gönderildiği veya saklandığı şekliyle alındığında emin olunması.
- Örnek: MD5, digital imza, anti-virus yazılımları.

Meşru kullanıcıların, anormal işletme şartlarında bile ağ elemanlarını, servisleri, uygulamaları kullanabilme yetkisinin belirlenmesi.

Örn: IDS/IPS, network redundancy, BC/DR (İş sürekliliği/Felaket kurtarma)

Availability (Kullanılabilirlik)

Privacy (Gizlilik)

Kimlik Tanımlamanın ve ağ kullanımının gizli tutulduğundan emin olunması.

- Örnek: NAT, Kriptolama

Güvenlik Mekanizmaları

Güvenlik servislerinin gereğini yerine getirmek için kullanılan yöntemlerdir.

- **Şifreleme Mekanizmaları(Encipherment Mechanisms)**

• veri gizliliği hizmet verirler.
• Asimetrik / Simetrik algoritmalar

- **Sayısal İmzalar (Digital Signatures)**

• Islak imzanının, elektronik ortamdaki sayısal eşdeğeridir.
• Genellikle asimetrik şifreleme uygulanır.

- **Erişim Kontrol Mekanizmaları (Access Control Mechanisms)**

• Doğrulanmış kimlik bilgilerini kullanarak , bir varlığa veya varlıkla ilgili bilgilere erişim kontrol hizmetlerinin sağlanması.

- **Veri Bütünlüğü Mekanizmaları (Data Integrity Mechanisms):**

• Veri bütünlüğünün sağlandığını kanıtlamak için, değişik ispat algoritmalarını kullanmak.
• Mesaj kimlik doğrulama kodları (MAC), dijital imzalar v.b

- **Kimlik doğrulama mekanizmaları (Authentication Mechanisms):**

• Temel bir kimlik temini, kimlik doğrulama hizmetleri sağlanması.
• Ortak anahtar altyapısı (PKI - public key infrastructure) gibi şifreleme teknikleri ve güven altyapısı dayanarak.

- **Trafik-Dolgu Mekanizmaları (Traffic-Padding Mechanisms)**

• Trafik analizi saldırılarına karşı koruma sağlama

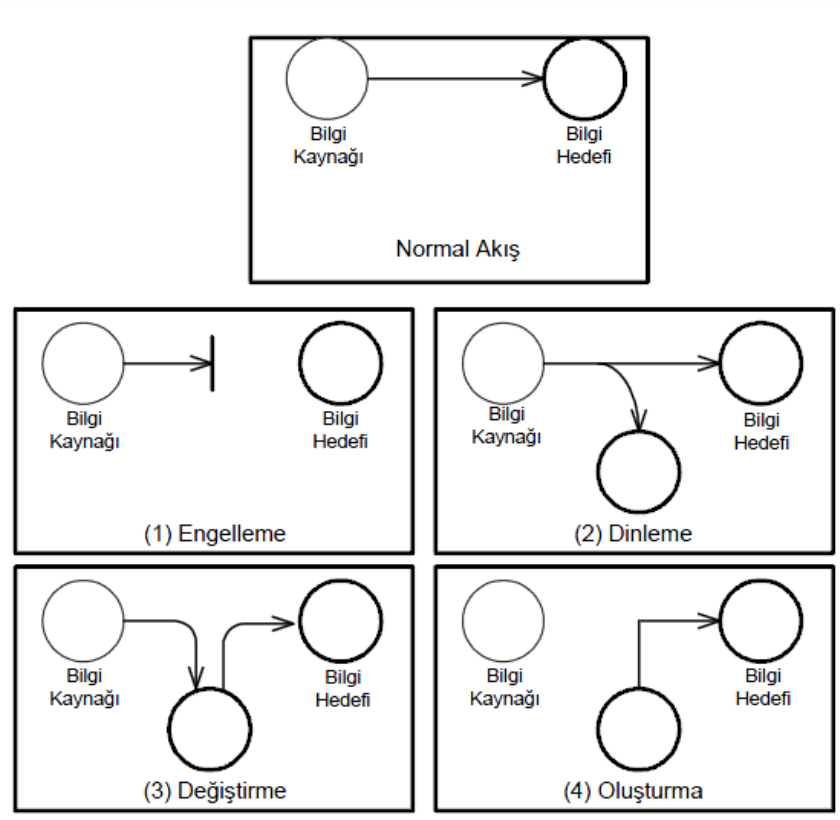
- **Yönlendirme Kontrol Mekanizması(Routing Control Mechanisms)**

• Belirlenmiş yollardan dinamik veya statik olarak, iletişim veri için belirli bir güzergah seçimi izini.

Saldırıların Sınıflandırılması

Süreçsel Sınıflama: Ağdaki veri transferiyle ilgili olarak güvenlik sorunları 4 kategoride incelenir.

1-Engelleme
2-Dinleme
3-Değiştirme
4-Oluşturma

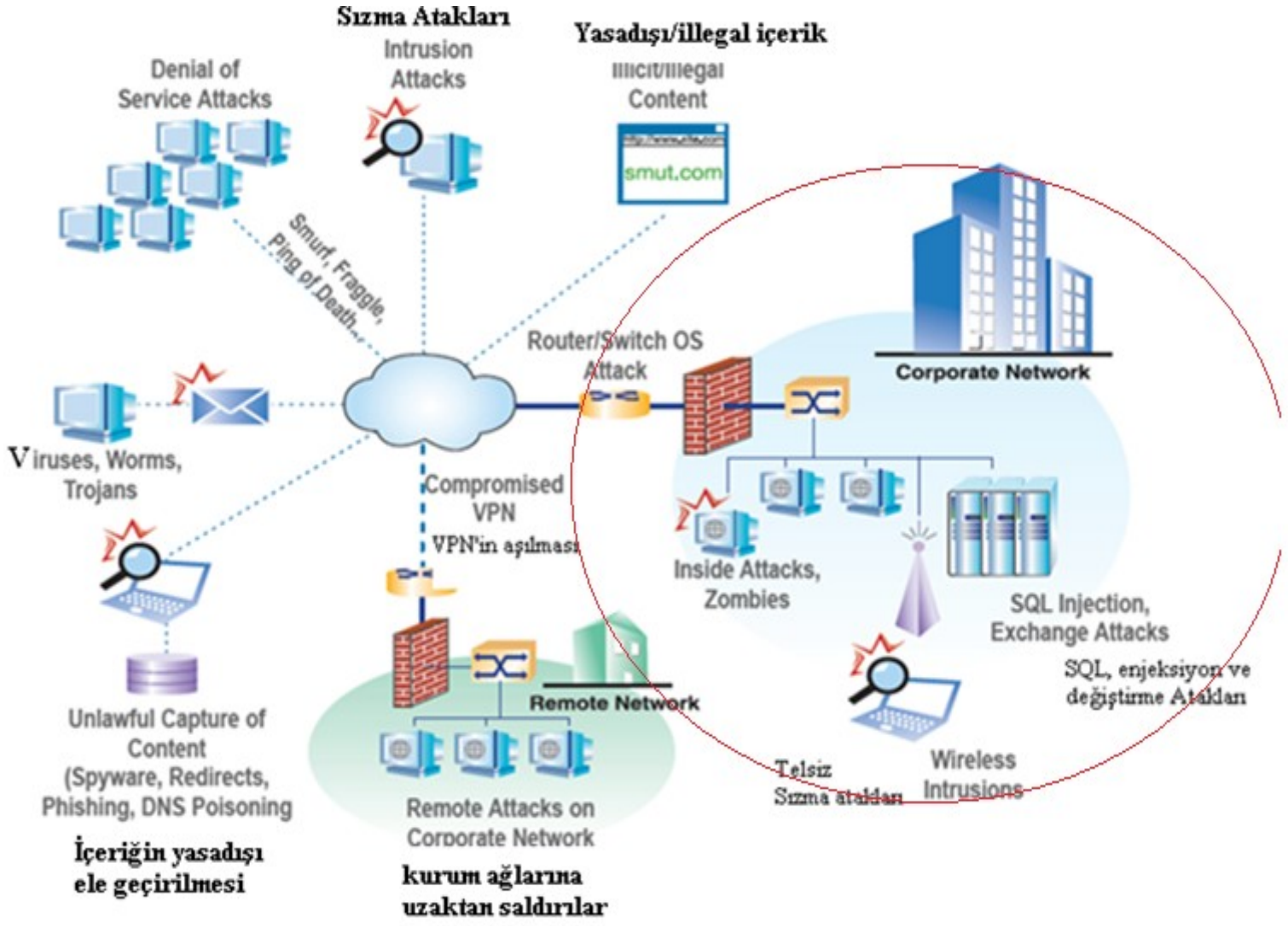


BMÜ-457 Ağ Güvenliği Dersi (2020-21Güz)

2.Hafta

Ağ Güvenliğine genel bakış

Günümüz ağ ortamında yaygın tehditler



Denial of Service Atakları

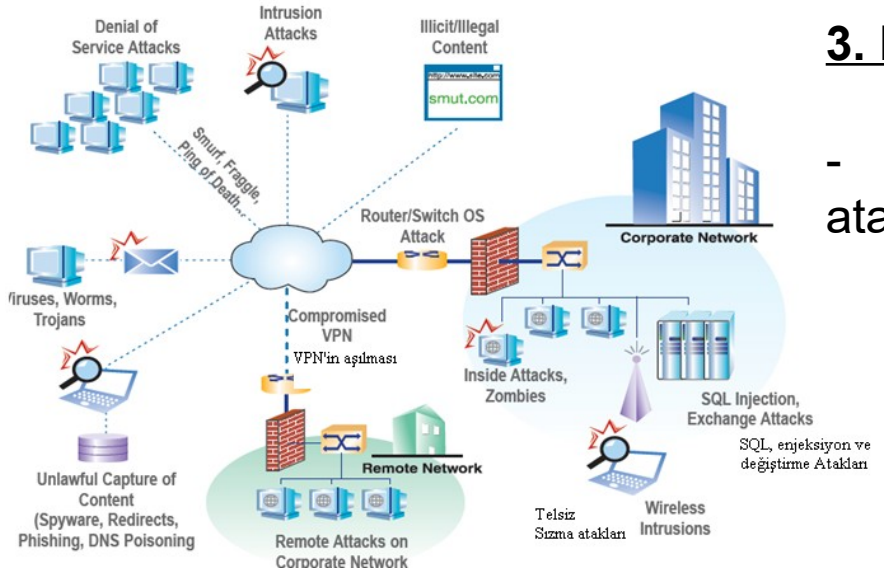
DoS (Denial of Services - Servis Dışı Bırakma) atakları temel olarak sistem kaynaklarını veya bant genişliği tüketerek servislerin hizmet dışı bırakılmasıdır. Bu atakların amacı bilgiyi çalmak değildir. Bu atakları 3 başlıkta toplamak mümkündür.

1. DoS - Denial Of Service :

-Paket direk olarak hedef sistem gönderilir.
-Tek bir kaynaktan tek bir hedefe yöneliktir.

2. DDoS - Distributed Denial of Service :

-Zombi kaynaklardan tek bir hedefe çoklu ataklardır.
-Anlık gönderilen paket sayısı zombilerin sayısı ile doğru orantılıdır.
-Çoğunlukla saldırıyı yapan kaynak tespit edilemez.



3. DRDoS - Distributed Reflective DoS:

- DDoS'tan farklı olarak daha sık ataklar için ek ağlar kullanır

4 çeşit temel DoS atağı vardır:

1. TCP/IP uygulamasındaki kusurları istismar eden ataklar: Örneğin Ping of Death ve Teardrop.

Ping-of-Death :Çok büyük boyuttaki (genelde 65,536 byte-ayarlanarak) ICMP paketleri direk olarak hedefe gönderilir. Paketin büyüklüğüne göre sistemin donmasına, çökmesine yada reset atmasına sebep olabilir.

TearDrop :Parçalanmış UDP paketleri bozuk ofsetler ile hedefe gönderilir. Hedef paketleri tekrar birleştirmeye çalıştığında bozuk veya hatalı bir paket üretmiş olur ve sistem çöker.

2. TCP/IP'deki zayıflıkları kullanan ataklar. Örneğin SYN Flood ve LAND atakları.

SYN Flood :TCP'nin 3 yollu handshake açığını kullanır. Kaynak (Saldıran) SYN paketlerini hedefe gönderir.(1. el sıkışma) . Hedef SYN paketine SYN ACK olarak cevap verir (2. el sıkışma). Saldıran (Kaynak) gelen pakete cevap vermeden yeni bir SYN paketi yollar ve hedef sürekli cevap bekler konumda kalır.

Land Attack :Kaynak ve Hedef adresi değiştirilmiş paketlerdir. Paket içerisindeki kaynak ve hedef gönderilecek hedef adresidir. Paket hedefe ulaştığında hedef kendi paketini sürekli cevaplayarak çöker.

3. Brute-force (Kaba kuvvet) atakları: Web yazılımlarının login kısımlarına yapılan deneme yanılma yöntemidir. Bu işlem yazılmış olan programları kullanılarak otomotik bir şekilde yapılır. Sürekli login sayfasına atak yapılarak deneme yanılma yöntemiyle bir kullanıcı adına ait şifreyi bulmak ve yönetimi ele geçirmektir. Bu tip ataklar networkü gereksiz data ile istila ederler. Örneğin Smurf atağı.

Smurf :ICMP paketlerindeki kaynak adresi değiştirir. ICMP paketlerini zombilere gönderir. Zombiler paketleri hedefe yollar. Hedef kendisinin göndermediği bir sürü cevap mesajları alarak şişer.

4. IP Spoofing (IP Sahtekarlığı) : Sistemlere girmek için, saldırganın kimliğini gizleyebilmesi için veya DoS atağının etkisini büyütmek için kullanılır. Saldırganın kendisini gizleyebilmesine sebep olan şey, HTTP, DNS gibi Internet servislerinde, IP numaralarını doğrulayacak bir denetim (authentication) bulunmamasıdır. IP spoofing'de, saldırgan, IP paketlerine kendi gerçek IP numarası yerine, var olmayan bir IP numarasını veya kurban sitenin numarasını koymaktır. Zombiler veya kurban siteler bu paketlerdeki gönderen IP numarasını doğrulayamadıkları için saldırgan kendisini gizleyerek istediği siteye saldırabilmektedir. Bu saldırının temel alındığı DDoS saldırıları **SYN-flood , smurf** v.b

İntrusion Attacks (Sızma Atakları)

Bir ağ ortamında, ağ kaynaklarına izinsiz erişim yapan veya yapmaya çalışan, sistemi kötüye kullanan kişiler saldırgan kapsamındadır. **Bunlara cracer veya hacker denir.**

Saldırısını sonuçlandırarak sisteme girmeyi başaran saldırgana ise sızan-nüfüz eden (intruder) olarak tanımlanır. Sızma işleminin sonucunda; sistemde yetkisiz kullanım, kaynaklara izinsiz erişim, bilgi çalınması, sadece sistemi meşgul ederek servis dışı kalması gibi kötü olaylar oluşur.

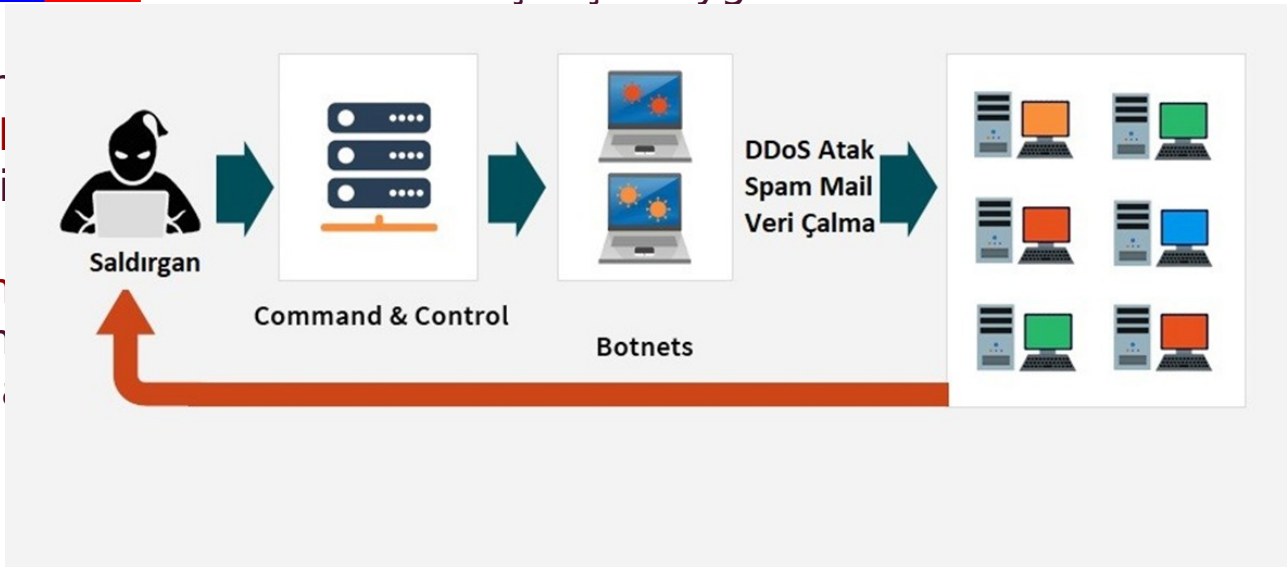
Sisteme sızma için gerçekleştirilen ataklara ise intrusion attacks (Sızma Atakları) denir.

BOTNET (roBOTNETwork)

Botnet, hacker tarafından, trojanlar'ın çeşitli ve çok sayıda bilgisayar sistemlerine bulaştırılarak bu bilgisayardaki yetkilere sahip olması olarak tarif edilebilr. Bir botnet trojanı sisteme bulaştıktan sonra artık o bilgisayar bir zombiye dönüşerek botnet ağının bir üyesi olmuştur ve botnet ağ yöneticisinin her istediğini yapmaya hazır hale gelmektedir. DDOS için kullanılan Botnet virüslerin CPU kullanımları fazla olmadığı için kullanıcı tarafından fark edilmez. Botnetteki her bilgisayar bir BOT veya Zombi'dir. Botnet ağındaki tüm zombiler, sadece bir bilgisayardan (hacker) komut verilerek yönlendirilir.

Botnet'ler, DDOS Saldırıları için çok uygundur.

•Zom
•Uzal
•Sahi
•Her
•Tüm
•Tüm
yazıl



AĞ güvenliğine katmanlı bakış

Güvenlik seviyesi Security level	Uygulanabilir güvenlik önlemleri Applicable security measures
1. Perimeter (Geniş kapsamlı - Çevresel)	• Firewall **(Ateş duvarı)** • Network-based anti-virus **(Ağ temelli anti-virüs)** • VPN encryption **VPN şifreleme**
2. Network	• Intrusion detection/prevention system (IDS/IPS) **(Saldırı tesit/Önleme Sistemi)** • Vulnerability management system **(Güvenlik açığı yönetim sistemi)** • Network access control **(Ağ erişim kontrolü)** • Access control/user authentication **(Erişim kontrol/Kullanıcı kimlik doğrulaması)**
3. Host	• Host IDS **(Host saldırı tespit sistemi)** • Host vulnerability assessment (VA) **(Host güvenlik açığı değerlendirmesi)** • Network access control **(Ağ erişim kontrolü)** • Anti-virus **Anti-virüs** • Access control/user authentication **(Erişim kontrol/Kullanıcı kimlik doğrulaması)**
4. Application	• Application shield **(Uygulama koruması)** • Access control/user authentication **(Erişim kontrol/Kullanıcı kimlik doğrulaması)** • Input validation **(Giriş Doğrulama)**
5. Data	• Encryption **(Kripto)** • Access control/user authentication **(Erişim kontrol/Kullanıcı kimlik doğrulaması)**

Güvenlik Seviyelerine katmanlı bir yaklaşım ve her katmanda uygulanacak teknolojik fonksiyonlar.

Firewall - Güvenlik duvarı

- Firewall - Güvenlik duvarı, genellikle bağlı bir sunucu üzerinde yüklü bir yazılımdır veya donanımsal bir kutudur.
- İç ve dış ağı biribirnden ayıran noktadır. Genellikle iç ağı dış ağdan korur.
- Güvenlik duvarı üç genel işlevleri gerçekleştirir;
  1) Trafik kontrol,
  2) Adresi çevirisi (NAT),
  3) VPN (Virtual Private Network) sonlandırma.

Özel Sanal Ağ (Virtual private network (VPN))

- VPN - Sanal özel ağ (VPN), dizüstü bilgisayarlar, ve hedef ağ gibi uzak cihazlar arasında güvenli bir bağlantı oluşturmak için yüksek düzey bir şifreleme tekniği kullanır.
- Aslında özel ağın güvenliğine ve gizliliğine yaklaşılan bir uygulamadır. Internet(Genel bir ağ) üzerinden şifreli bir haberleşme şekli olarakta düşünülebilir.
- VPN tüneli, DMZ içinde bir VPN-etkin yönlendirici, güvenlik duvarı, ya da sunucu üzerinden sona erdirilir.

LEVEL 5: DATA SECURITY (Veri Güvenliği)

- Network'te seyahat eden Şifrelenmiş veri diğer güvenlik önlemleri aşılmış olsa bile güvenlik sağlayan bir yöntem olarak görülebilir.
- Güçlü şifreleme programı, özel verileri korur.
- Veri güvenliği, organizasyon çapındaki güvenlik politikalarına son derece bağımlıdır.
- Verilere erişimi kimin idare edeceği, kullanıcılar hangi yetkilere sahip olacağı, kendi bütünlüğü v.b
- Şifreleme , erişim kontrol / Kimlik doğrulama teknolojileri bu sevide koruma işlemi yapan teknoloji…

- Veri şifreleme programları yaygın olarak , veri, uygulama ve işletim sistemi seviyelerinde uygulanmaktadır.
- Tüm şemalarda, veriye erişebilmek için şifreleme / şifre çözme anahtarlarını gerekir.
- Ortak şifreleme stratejileri PKI, PGP, RSA

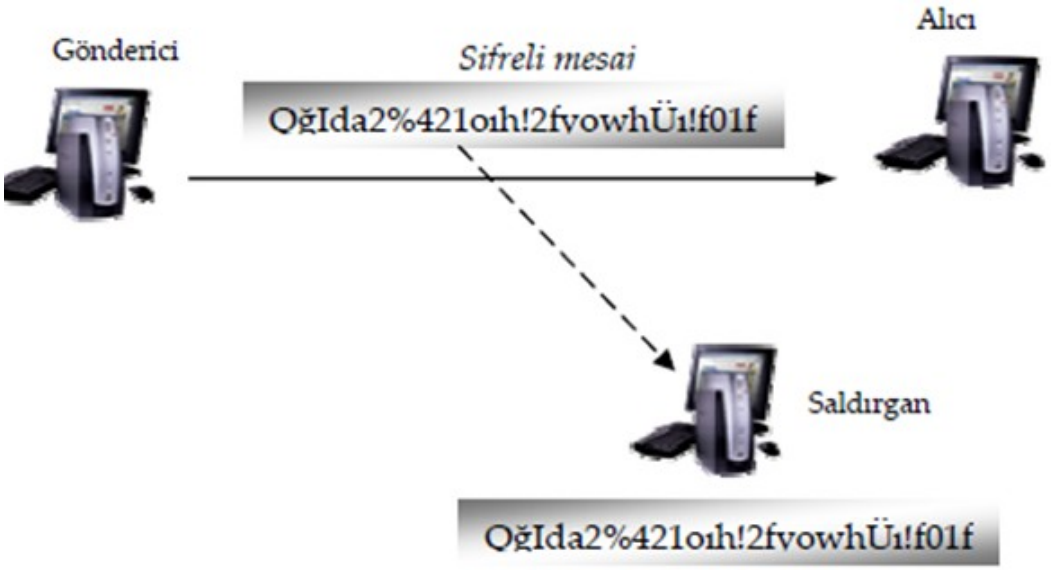
Kriptografi (Şifreleme)

- Kriptografi, veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılan bir teknolojidir.
- Şifreleme, iletişim sırasında verinin güvenliğini sağladığı gibi, değiştirilmesini önleyici bir tedbirdir (İçerik tabanlı koruma). Şifreleme de veriler şifrelenerek anlamsız hale getirilip hedefe gönderilir. Hedefte ise tam tersi işlem yapılarak (Deşifreleme) orijinal haline çevrilir.
- Aşağıda bazı açık metin(Clear text) kullanan protokollar görülmektedir.

- FTP Doğrulama açık metindir.
- Telnet Doğrulama açık metindir
- SMTP posta mesajlarının içeriği açık metin olarak dağıtılır.
- http Sayfa içeriği ve formlardaki bilgilerin içeriği açık metin olarak gönderilir.
- IMAP Doğrulama açık metindir
- SNMPv1 Doğrulama açık metindir

•Şifreleme, bu açıkları büyük ölçüde giderebilir.

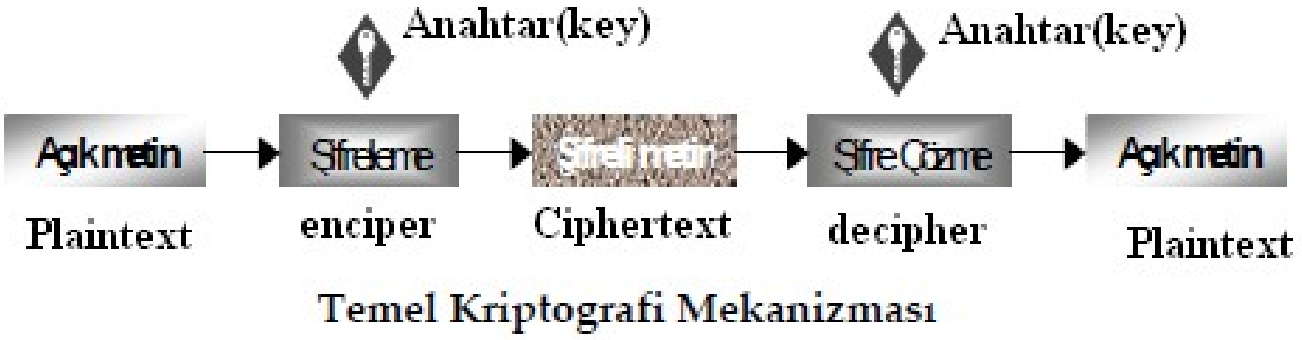
- Kripto sistemleri,Gizlilik, Veri Bütünlüğü, Kimlik Sınaması ve İnkâr Edememe hizmetlerinde kullanılır.



Hattı Dinleyen Bir Saldırgana Karşı Şifrelemenin Kullanılışı

Şifreleme

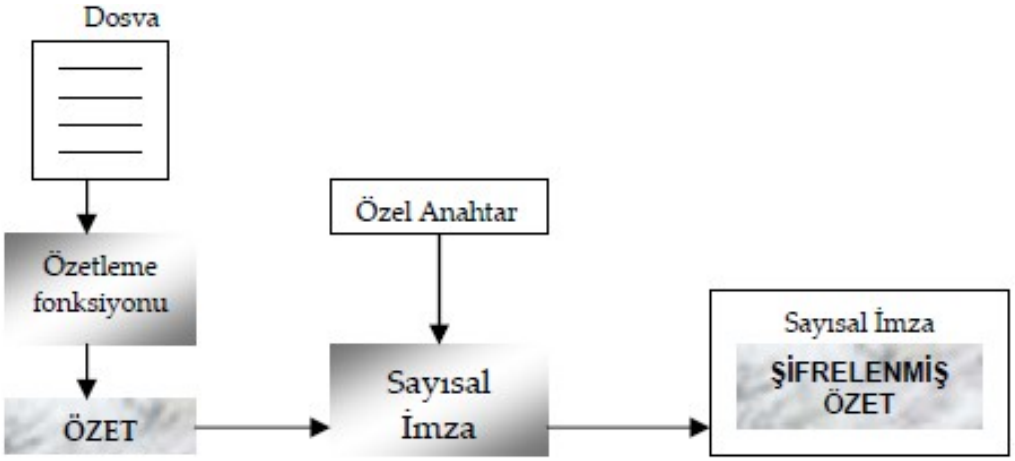
- **Kriptografi'de veri, matematiksel yöntemler kullanılarak kodlanır ve başkalarının okuyamayacağı hale getirilir. Bu matematiksel kodlamaya "*kripto algoritması*" adı verilir.**
- **Bir şifreli haberleşme için mekanizma aşağıdakilerden oluşur.**
- **1-Şifreleme Algoritması**
- **2-Deşifreleme Algoritması**
- **3-Anahtar**



Temel Kriptografi Mekanizması

Sayısal İmza ve PKI

- Sayısal imza , Kimlik Sınaması ve Veri Bütünlüğü prensiplerinin gerçekleştirilmesinde kullanılırlar (İçerik Tabanlı Güvenlik).
- Bir sayısal imza, şifrelenmiş bir özet (hash) değeridir. Sayısal imzalar yardımıyla, alıcı taraf göndericinin kimliğinin sınamasını yapar ve göndericinin kim olduğundan tam olarak emin olur.
- Bunun yanında, sayısal imza teknolojisi, gönderilen verilerin bütünlük sınamasında da kullanılabilir.
- Sayısal imzalar, gerçek hayatta kullanılan ve elle atılan imzanın (ıslak imzanın) bilişim dünyasındaki karşılığı olarak görülebilir.
- Bir sayısal imza, imzaladığı içeriğin, imzalandığı andan itibaren değişmediğinin kanıtlanmasında kullanılabilir



Bir Mesajın Sayısal İmzası'nın Oluşturulması

BMÜ-471 AĞ GÜVENLİĞİ

3.Hafta - OSI MODELİ KATMANLARI AÇIKLAR-SALDIRILAR-ÖNLEMLER

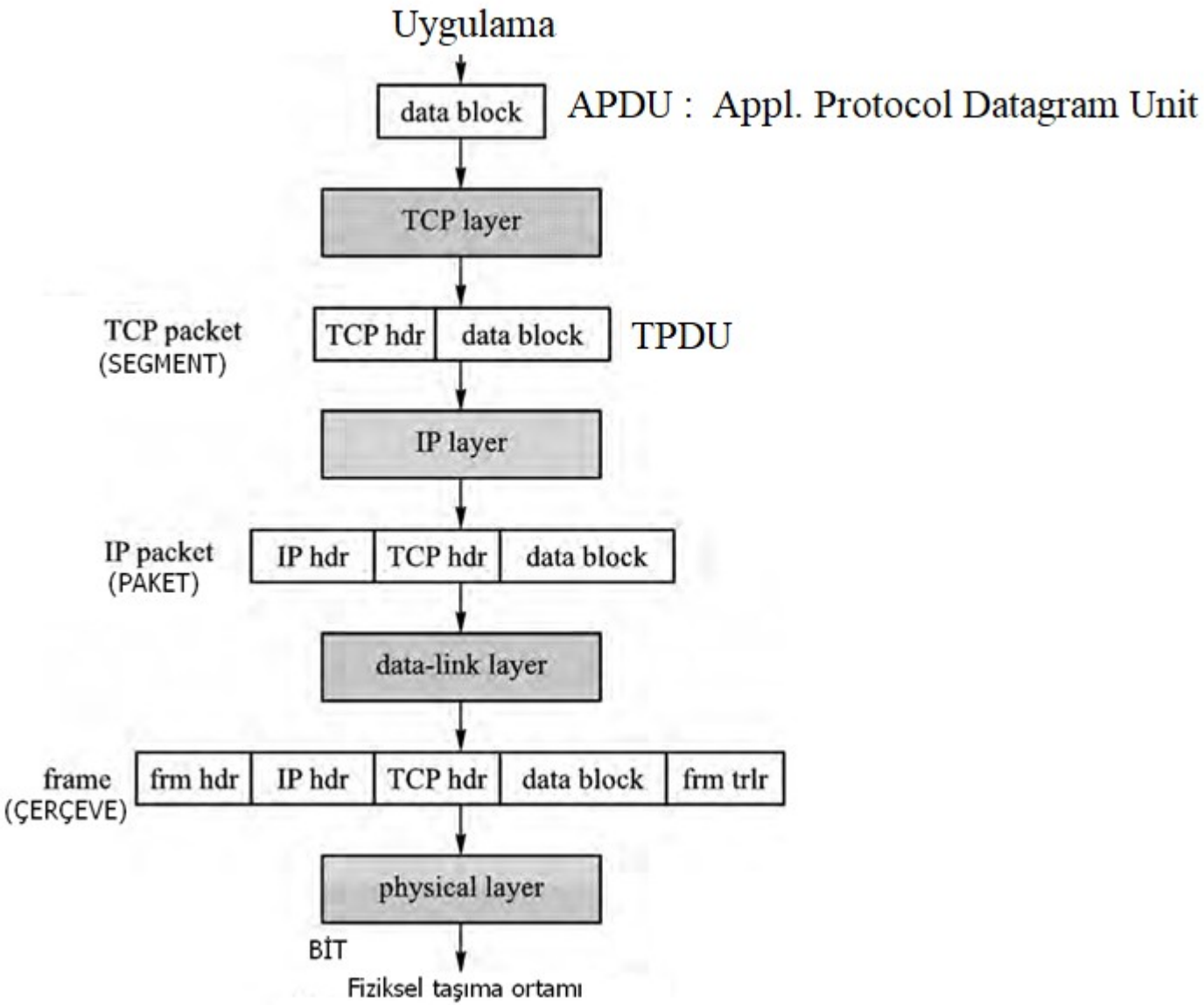
Bilgisayar Ağlarında Katmanlı Modelleme açısından Güvenlik

- Bilgisayar ağlarında güvenlik konusu, ağ bilgisayarlarındaki ve iletişim halindeki verinin Gizlilik, Bütünlük, İnkar edememe ve kullanılabilme özelliklerini bozmak için yapılan (illegal olarak) erişme, değiştirme, okuma, bütünlüğünü bozma, inkar etme, engelleme v.b saldırılarını önlemektir.
- Bu saldırılar, **ağ iletişim protokollarının açıklarından, ağ cihazları ve iç/dış ağ erişiminin tam olarak denetlenememesinden,** güvenlik politikalarının iyi oluşturulamamasından kaynaklanmaktadır.
- Özellikle TCP/IP iletişim protokol kümesiyle çalışan internet gibi dinlenmeye çok müsait ağ yapılarında seyahat eden verilerin hertürlü saldırıya açık olduğu bilinmektedir.
- Ağ güvenliği konusu üç farklı segment'te incelenecektir.

  1- İletişim protokolları açıklarından yararlanarak yapılan saldırılar ve tedbirler.

  2- Güvenlik protokollarının yapısı uygulanması

  3- Erişim güvenlik (İç ağ/Dış Ağ koruma)
- Bu derste TCP/IP ve OSI katmanlı ağ modeli ve ilgili katman protokolları ve bunların zayıflıkları üzerinde durulacaktır. Bu zayıflıklardan yararlanılarak yapılacak saldırılar ve tedbirleri nelerdir?
- İlgili ağ cihazlarının korunması ve cihazların uygun konfigürasyonları ile ağ güvenlik açıklarının azaltılması üzerinde durulacaktır.


Uygulama
data block
APDU : Appl. Protocol Datagram Unit
TCP layer
TCP packet
(SEGMENT)
TCP hdr
data block
TPDU
IP layer
IP packet
(PAKET)
IP hdr
TCP hdr
data block
data-link layer
frame
(ÇERÇEVE)
frm hdr
IP hdr
TCP hdr
data block
frm trlr
physical layer
BİT
Fiziksel taşıma ortamı

Veri bağı katmanı Protokolları

Veri Bağı katmanı protokoları, LAN ve WAN ağ yapıları için farklı farklıdır. Saldırı ve açıklar ve güvenlik protokollarının'da LAN veya WAN DLL protokollarına göre incelenmesi uygundur.

En çok kullanılan Veri bağı LAN protokolları

- Ethernet
- Token Ring
- FDDI

Sık kullanılan WAN veri bağı protokolları

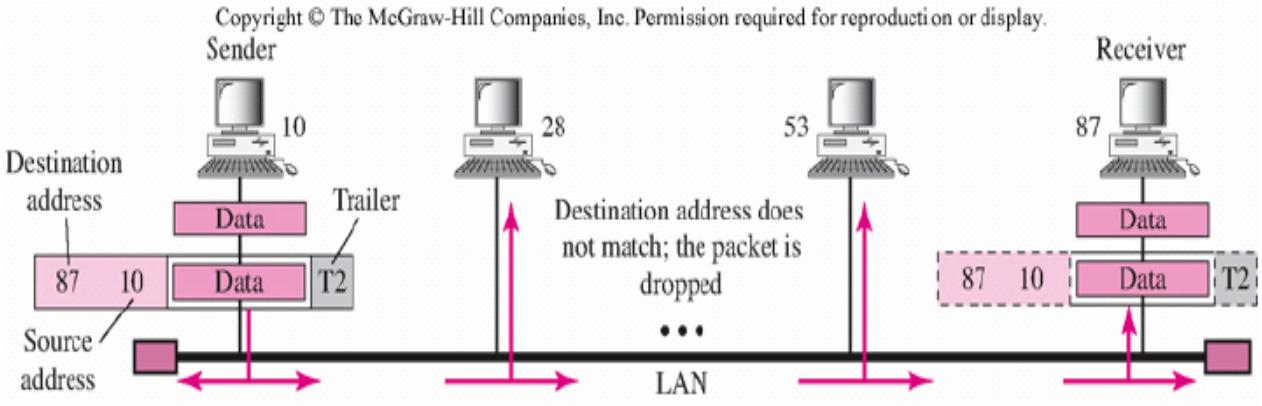
- PPP (point to point protocol)
- HDLC (High Level Data Link Control)
- Frame Relay
- ATM (Asychronus Transmısion Mode)

Fiziksel Adresleme

- Bir Ağ içerisindeki iki bilgisayarın biribirleriyle haberleşebilmesi için Fiziksel Adreslerinin bilinmesi gerekir.
- Fiziksel adresler ağdaki cihazların değişmez gerçek adresleri olarak tarif edilir. NIC kartlarının belleklerinde yazılırlar. Ethernet teknolojisinde 48 bit uzunluğunda (Media Acces Control – MAC)dır.
- Bu adresleme DLL katmanında kullanılır. Aynı ağ içerisinde bu adreslemeye göre çerçeveler yerine ulaşır.

Fiziksel adresleme

- Data link layer'da frame içinde bulunur. Ağ yapısına göre farklı uzunluktadır. (Ethernet için 6 byte NIC, LocalTalk Apple için 1 byte)

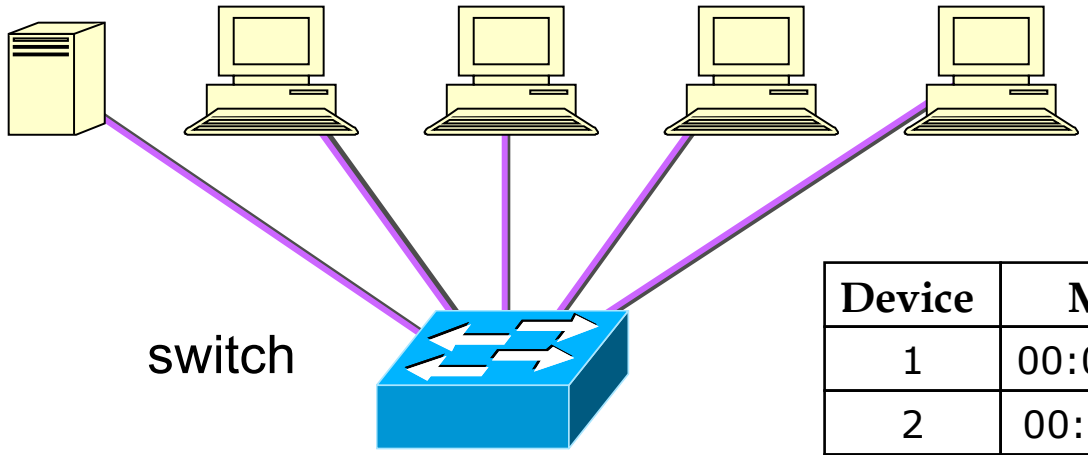


Swithc'ler

Switchler 2. katmanda paket süzme işlemi;

- *Hangi MAC adresinin switc'hin hangi portunun arkasında olduğunun öğrenilmesi.*
- *Paketi sadece uygun porta geçirme işlemi.*

L2'de çalışan Switchler, portları arasındaki iletişimi üzerlerindeki MAC adres tablolarına bakarak yapar. MAC adres tablosunda (CAM tablosu); port numarası, porta bağlı olan bilgisayar(lar)ın MAC adres(ler)i ve ilgili portun hangi VLAN'e ait olduğu gibi bilgiler yer alır.



10/100BASE-T

Device	MAC address
1	00:0e:81:10:19:FC
2	00:0e:81:32:96:af
3	00:0e:81:31:2f:d7
4	00:0e:81:97:03:05
8	00:0e:81:10:17:d1

İkinci Katman Saldırıları (LAN için)

•Ağ saldırıları denince öncelikle OSI'nin üçüncü (Ağ Katmanı) ve daha yukarı katmanlarıyla ilgili ataklar akla gelmektedir. Ağ yöneticileri, ikinci katman saldırılarına pek yoğunlaşmazlar, çünkü harici hakerların ilgili cihazlara erişiminin zor olduğu düşünülür. Bu tedbirsizlik, ağ cihazlarına kolay ataklar yapmakla sonuçlanır. Veya bu katmanla ilgili protokolların açıklarından faydalanılarak gerçekleştirilir. Dolayısıyla ikinci katman saldırıları en az üst katmanlara yönelik yapılan ataklar kadar etkili olabilmektedir.

• İkinci katman atakları yerel alan ağlarının içinden (LAN) yapıldığı için güvenlik duvarı ya da saldırı engelleme / tespit etme sistemleri tarafından engellenememekte/tespit edilememektedir. Çünkü bu sistemler genellikle üçüncü ve daha üst katmanların güvenliği için tasarlanmıştır. Dış ağdan iç ağa gelecek saldırıları tespit veya engellemek için kullanılırlar.

•Ağ güvenliği tüm OSI katmanlarının güvenliğinin ele alınmasıyla asıl amacına ulaşacaktır. Üst katmanların güvenliğinin alınıp, ikinci katman güvenliğinin ele alınmaması ağ güvenliğinin tam anlamıyla anlaşılamadığını gösterir.

1. MAC Adres Atağı

- Anahtara gelen çerçevenin hedef MAC adresi, anahtarın MAC adres tablosunda bulunmadığı durumlarda, anahtar çerçeveyi (frame) tüm portlarına yollayacaktır. Peki bu nasıl gerçekleşir?

- Anahtarın MAC adres tablosunun tamamen dolu olduğunu düşünelim. Switchin beşinci portuna bağlı bir bilgisayardan gönderilen çerçevenin (frame) hedef MAC adresinin, anahtarın MAC adres tablosunda bulunmadığını düşünelim. Bu durumda anahtar, beşinci portundan gelen çerçeveyi (frame) diğer tüm portlarına yollayacaktır. Bu işlem ilgili beşinci porttan çıkan tüm bilginin diğer portlara da gönderilmesi sonucunu doğuracaktır.

- Bu da saldırganın, anahtar üzerinde herhangi bir port yönlendirmesi yapmadan, sadece anahtarın MAC adres tablosunu sahte MAC adresleriyle doldurmak suretiyle, anahtar üzerindeki tüm trafiği dinleyebilmesine yol açacaktır. ***Ayrıca anahtarın performansı da düşecektir.***

Anahtarın MAC adres tablosunu sahte MAC adresleriyle doldurabilecek yazılımlar mevcuttur. Anahtara bu yazılımlar ile saldırılıp MAC adres tablosu sahte adreslerle doldurulabilir. Bu saldırıdan sonra anahtarın MAC adres tablosu aşağıdakine benzer bir durumda olacaktır. Saldırganın portunun GigabitEthernet 3 /33 olduğunu düşünüyoruz.

vlan	mac address	type	protocols	port
20	000a.2281.61e4	dynamic	ip	GigabitEthernet 1/1
20	000a.2201.9079	dynamic	ip	GigabitEthernet 1/1
20	000a.22c0.ddf9	dynamic	ip	GigabitEthernet 1/1
61	001b.2461.09f6	dynamic	ip	GigabitEthernet 1/2
61	0040.ca79.8821	dynamic	ip	GigabitEthernet 1/15
61	00d0.b7bc.3d2c	dynamic	ip	GigabitEthernet 3/34
61	0800.8e05.1bbc	dynamic	ip	GigabitEthernet 3/33
61	0800.8e05.1aaa	dynamic	ip	GigabitEthernet 3/33
61	0800.8e05.1aab	dynamic	ip	GigabitEthernet 3/33
61	0800.8e05.1aac	dynamic	ip	GigabitEthernet 3/33
61	0800.8e05.1aad	dynamic	ip	GigabitEthernet 3/33
61	0800.8e05.1aae	dynamic	ip	GigabitEthernet 3/33
61	0800.8e05.1aaf	dynamic	ip	GigabitEthernet 3/33
61	0800.8e05.1ab0	dynamic	ip	GigabitEthernet 3/33
61	0800.8e05.39b7	dynamic	ip	GigabitEthern 3/35

ÇÖZÜM:

- Bu saldırıdan korunmanın yolu çok basittir: MAC adresi kilitlemesi (belirli bir MAC adresini kayıtlı bir IP adresine eşleştirme). Ancak bunun için elimizdeki anahtarın MAC adres kilitlemesi özeliğinin olması gerekmektedir.
- Anahtarlarımızın portlarına MAC adresi kilitlemesi uygularsak bu olası saldırıdan kurtulmuş oluruz. Aşağıda Cisco anahtarlar için MAC adresi kilitlemesi örnek konfigürasyon satırları bulunmaktadır:
- (Aşağıdaki konfigürasyonlar sizin sistemlerinize uygun olmayabilir.)
- **CISCO konfigürasyonu**
- Anahtar(config) # interface range GigabitEthernet 3/2 – 48
- Anahtar(config-range) # switchport mode access
- Anahtar(config-range) #switchport mode security
- Anahtar(config-range)# switchport port-security maximum 3
- Anahtar(config-range)# switchport port-security violation restrict (ihlal kısıtlaması)
- Anahtar(config-range)#switchport port-security mac-address sticky

2. Sahte MAC (MAC Spoofing) Atağı

- Bu atak türünde saldırgan, anahtara gönderdiği çerçevelerin (frame) içerisindeki “kaynak MAC adres” kısmına, dinlemek istediği bilgisayarın MAC adresini yazar.
- Anahtar MAC adres tablosunu bu duruma göre günceller. Böylece anahtarın MAC adres tablosunda, saldırganın bağlanmış olduğu anahtarın portu için iki adet MAC adresi yer almış olur. (Saldırganın MAC adresi ve hedef bilgisayarın MAC adresi) Hedef bilgisayara gönderilen çerçeveler de (frame) de böylece saldırganın bilgisayarına gönderilmiş olur.
- Hedef bilgisayar ağa paket gönderene kadar bu durum devam edecektir.

IP Adresten Ethernet Adresine dönüş

- Address Resolution Protocolü (ARP)
  - 3.katman protokolüdür.
  - IP adreslerin MAC karşılıklarını haritalar.
  - Ağ katmanı, bir çerçeve hazırlanırken ARP'yi kullanır.
- ARP Sorgusu
  - 192.168.0.40 kimdir? 192.168.0.20 cevap verir.
- ARP Cevabı
  - 192.168.0.40 'nin MAC'ı 00:0e:81:10:19:FC
- ARP cache'ları hızlı çalışma için gereklidir.
- Önceki ARP cevaplarını kayıt eder.
- En eski sorgular silinir.

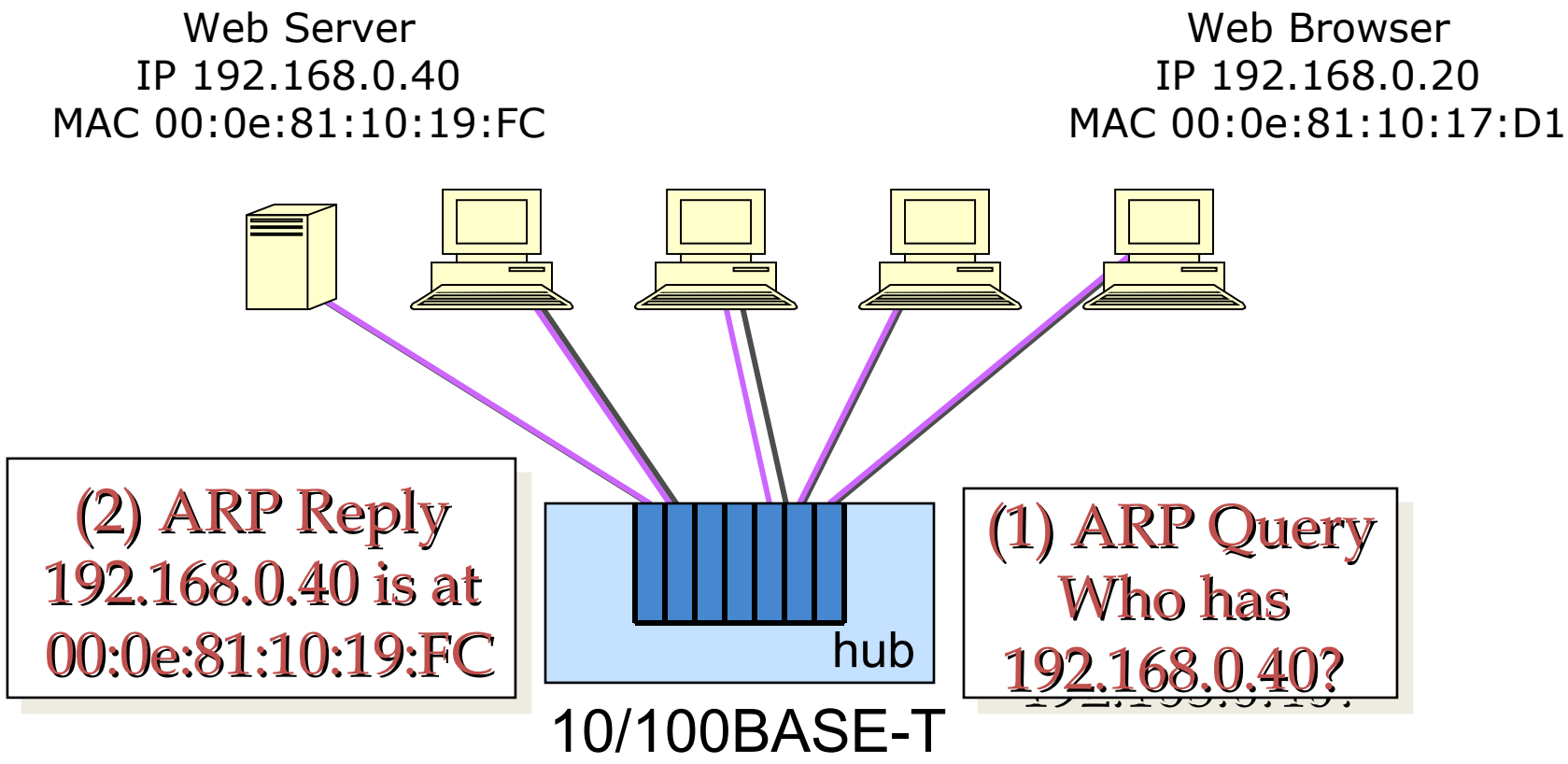
ARP PROTOKOLU VE YÖNELİK SALDIRILAR:

- Adres Çözümleme Protokolü (ARP) Fiziksel (Ethernet MAC) arayüz adresi ile ağ IP adreslerini eşleştirme için kullanılır.
- Veri bağı katmanında Broadcast yayın yoluyla işlem yapar.
- Bu protokolda ençok kullanılan ARP istek (Request) ve ARP Cevap (reply) paketleri'dir.
- Bilinen MAC adresine karşılık gelen IP adresi ise RARP protokolu ile gerçekleşir.
- RARP protokolu daha çok ağa bağlı fakat HARD Diskİ olmayan bilgisayarların ağa dahil olduktan sonra kendi IP No'larnı bulmak için kullanılan protokoldur. (HD'si olan bilgisayarlar kendi IP adreslerini kendi HD'leri üzerinde barındırılar))
- Bunun için ortamda RARP veritabanı tutucu bilgisayarlar olmalıdır.
- RARP protokolu sunucu-istemci etkileşimi ile çalışırlar.

ARP Sorgusu & ARP Cevabı

ARP tablosunu görmek için bilgisayarınızda "arp –a" komutu kullanılabilirsiniz.

```
C:\> arp -a
Arabirim: 192.168.1.70 --- 0x4
Internet Adresi      Fiziksel Adres          Tipi
192.168.1.1          00-02-xx-yy-ad-15       dinamik
192.168.1.253        00-0c-tt-zz-6b-5d       dinamik
```



ARP Güvenlik kusurları

ARP protokolunun işleyişi ve tasarım mekanizmasından dolayı önemli kusurlardan bazıları;

- ARP önbellekleri kapasitesinin sınırlı oluşu.
  ARP önbellekleri bir şekilde lüzumsuz olarak doldurulabilir.
- ARP Kimlik Doğrulama eksikliği
  - ARP cevapları, genellikle kabul edilen ve alınanın kim olduğu fazla önemsenmeden önbelleğe alınır.
  - Meşru ve gayri meşru mesajları ayırt etmek için hiçbir yöntem yoktur.

Kimli doğrulama eksikliğinden dolayı;

- Geçersiz ARP cevapları: Bir ARP sorgusuna ki bu bir broadcast yayındır. Alakasız kimseler cevap verebilir. Bu durumda sorgulanan IP'ye ilgisiz kiiler kendisini eşleştirebilir.
- Karşılıksız - Sebepsiz (Gratuitous) ARP cevapları:
  Sorgu olmadan, saldırganın yönlendireceği ağın eşleştirilmesini sağlayan ARP cevaplarının ön belleğe yazılabilir olması.

ARP Güvenlik Açıkları

- ARP spoofing (ARP Kimlik Sahtekarlığı- ARP taklidi)
  - Sebepsiz, nedensiz ARP işlemleri.
  - Orijini doğrulanmayan ARP yanıtları.
  - Kötü niyetli bir cihaz herhangi bir MAC adresini talep edebilir.

ARP Saldırıları

- ARP önbelleklerindeki mevcut adreslerin değiştirilmesi

ARP sahtekarlığı (ARP spoofing, ARP flooding, ARP poisoning) saldırısı lokal ağlarda gerçekleştirilebilen bir saldırıdır.Bu saldırı, üç şekilde gerçekleştirilmektedir:

- Birincisi; hedef bilgisayarın ARP tablosunun yanlış bilgilerle dolmasını sağlayarak, hedef bilgisayarın göndereceği paketlerin saldırganın istediği adreslere gitmesini sağlamak.
- İkincisi; hedef bilgisayarın göndereceği tüm paketlerin, saldırganın bilgisayarı üzerinden geçmesini sağlamak **(Man in the Middle).**
- Üçüncüsü de; hedef bilgisayarın, paketlerini bir başka bilgisayara göndermesini sağlayarak bu bilgisayara servis dışı bırakma **(Denial of Service)** saldırısı yapmak şeklindedir.

- ARP Önbelleğinin aşırı kalabalık olması

Bazı uygulamalardaki hedef, çok sayıda gereksiz ARP yanıtları gönderilerek ARP belleğinin doldurulmasıdır.

Bu durumda önbellek maksimuma erişir. Switchler ya HUB gibi çalışır. Veya tekrardan öğrenme moduna girer.

4. Sahte ARP (ARP Spoofing, ARP Poisoning) Atağı

- Normalde ağdaki bir bilgisayar, paket göndereceği başka bir bilgisayarın MAC adresini öğrenmek için anahtara ARP isteği (ARP request) paketi gönderir ve anahtar bu paketi tüm portlarına gönderir. Sadece paketin gönderileceği hedef bilgisayar bu ARP isteğine cevap verir. Paketi gönderen bilgisayar da bu IP – MAC eşleşmesini kendi ARP tablosunda tutar.
- Sahte ARP ataklarında saldırgan, paketin gönderileceği bilgisayarın yerine ARP isteğine cevap verir. Böylece paketi gönderen bilgisayarın ARP tablosunda (IP – MAC eşleşmesi tablosu) saldırgan bilgisayarının IP ve MAC adresleri bulunacaktır. Böylece hedefteki bilgisayar gönderilecek olan paketler saldırganın bilgisayarına gönderilir.
- Saldırgan varsayılan ağ geçidinin (default gateway) yerine ARP isteklerine cevap verecek olursa da, ağdan dışarı çıkacak olan tüm paketler, varsayılan ağ geçidi (default gateway) yerine saldırganın bilgisayarı üzerinden dışarı çıkacaktır. Böylece saldırgan hem ağdan çıkan tüm paketleri dinleyebilecektir hem de bilgisayarının donanım özelliklerine bağlı olarak ağda performans düşüklüğüne sebep olacaktır.

Paketlerin Monitor edilmesi (Sniffing)

- HUB'lar bir portundan gelen paketleri diğer paketlere broadcast yaparlar. Bunun anlamı aynı Hub'ı paylaşan bilgisayarların paketleri monitor etmesine sebep olur.
- Switch'ler ise gelen paketin ***"Hedef MAC adresini"*** inceleyerek o paketi yalnızca ilgili porta yönlendirirler. Bu iş için oluşturdukları ***"MAC Adresi-Port no***' tablolarını kullanırlar.
- Switch kullanılan ağlarda, bu sayede bilgisayarların biribirlerine giden paketleri monitor etme olasılığı bir ölçüde önlenebilir.
- Switchler her ne kadar dinlenmemek üzere tasarlansa da değişik yöntemlerle bu durum aşılabilir.
- Gelişmiş switchler'de (kontrol edilebilir SWitch'ler) bu dinlenme problemi aşılabilir.

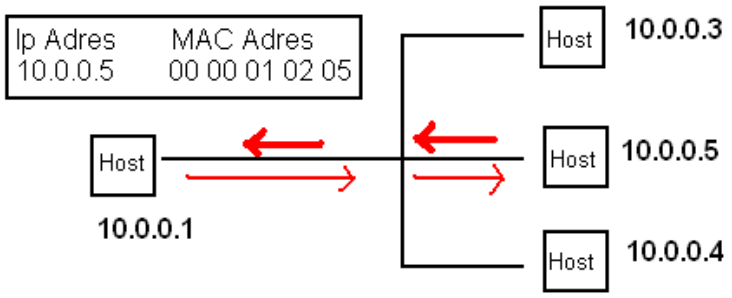
Paketlerin Monitor edilmesi (Sniffing)-II

- Gelişmiş olmayan switchler'in dinlenmesi için değişik yöntemler uygulanır. Bunlardan en önemlisi ARP Tablo(önbellek) zehirlenmesidir.
- ARP Tablo Zehirlenmesi (ARP SPOOFİNG – Cache Poisoning) : Bu yöntem, Ortadaki Sessiz Adam - Man in the Middle- saldırısı şeklinde etkisini gösterir.
- Saldıgan haberleşen iki bilgisayar arasına kendisini yerleştirerek bir köprü gibi veri akışının kendisi üzerinden sağlanmasını sağlar. Böylece gelen paketleri okuyan saldırgan paketleri iki makine arasında yönlendirir. Ortadaki adam ile DNS zehirlenmesi de yapılır.

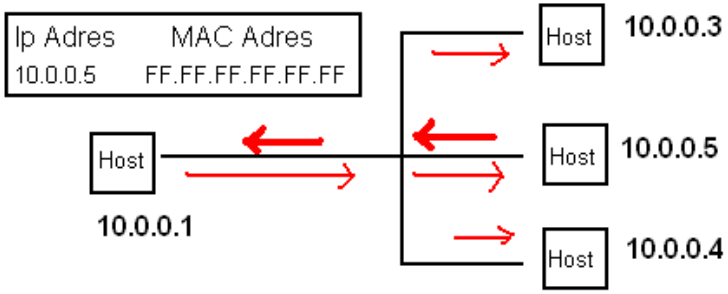
- **Man-in-the-Middle Saldırıları:** Bu tür saldırılarda saldırgan kurban ile kurbanın gitmek istediği hedef noktası arasına girerek bütün iletişimi istediği gibi kontrol eder. Bu saldırılar birçok değişik şekilde karşımıza çıkabilir.(ARP Zehirlenmesi, DNS Ön Bellek Zehirlenmesi vb.)

Toplu yayın (Broadcast) Saldırısı

- Eğer ARP tablosu içerisindeki belirli bir IP adresine karşılık gelen MAC adresi, ARP spoofing (taklit ARP yanıtı) mesajı yoluyla değiştirilip FF.FF.FF.FF.FF.FF ile değiştirilirse, bu bilgisayara gönderilecek paketler tüm noktalar tarafından monitör edilebilir okunabilir.
- Eğer bir bilgisayarın ARP tablosunun içindeki ağ geçidinin IP'sine karşıkıl gelen MAC adresi toplu yayın adresi olarak değiştirilirse, **bu bilgisayarın dış dünya ile olan bağlantısı** rahatlıkla izlenebilir.



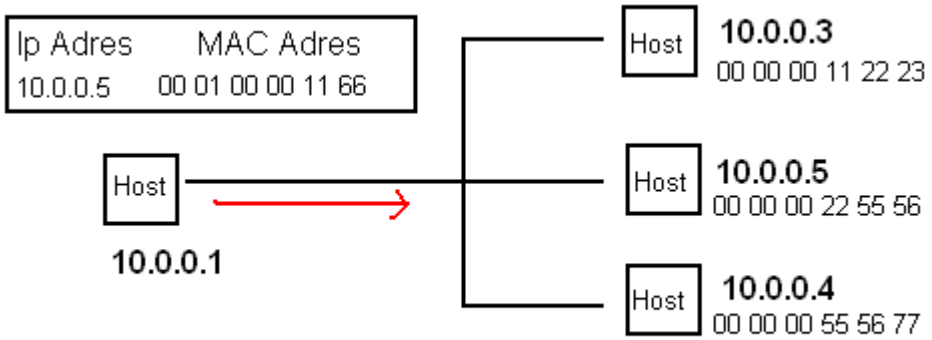
Toplu Yayın Saldırısı Öncesi



Toplu Yayın Saldırısı Sonrası

ARP PROTOKOLU İLE DOS Saldırıları

- Taklit edilmiş “ARP yanıt Paketi” kullanarak tablo içerisinde varolmayan MAC adresi değerlerine karşılık gelen IP adrteslerine sahip olan girdiler yapılır. Böylelikle tablo içerisinde yer alan IP adresine gönderilecek datagramlar hedeflerine varamaz. Bu durum ağı meşgul eder hem de MAC adresi değiştirilmiş bilgisayarla olan iletişim sonlandırılmış olur.



DOS Saldırıları

ARP SALDIRILARINA KARŞI ÖNLEMLER

Eski bir protokol olan ARP'ın çalışma yapısından *(Tablosunun düşük kapasiteli olması, ARP mesajları için herhangi bir durum tablosunun tutulmaması, ARP'ta herhangi bir kimlik doğrulama mekanizması olmadığı için, bilgisayar gelen ARP mesajlarının doğru bilgisayardan gelip-gelmediği kontrol edemeyecektir. Tüm bilgisayarlar kendisine gelen ARP mesajlarıyla ARP tablosunu herhangi bir kontrole tabi tutmadan güncellemek durumundadır v.b)* kaynaklanan bu sorunların protokol bazında bir çözümü bulunmamaktadır.

- Alınacak tedbirlerden ilki ARP tabloları içerisine statik girdiler yaratmaktır. Bu statik değerler saldırı sonucunda değişmeyeceği için belirli bir düzeyde güvenlik sağlanmış olur. Ancak bu yöntem ağdaki tüm bilgisayarların ARP tablolarına manuel olarak " IP-MAC adresi" tanımlaması yapmaktır. Mantıklı değildir. Kaldı ki Windows işletim sistemi, ARP tablosu içerisindeki statik eşleşmeleri kabul etmeyebilir. Aldığı Yanıt paketleri ile tabloyu değiştirebilir.

ARP SALDIRILARINA KARŞI ÖNLEMLER-2

- ARP' nin açıklarından yararlanılarak yapılan saldırıları SWİTCH cihazları üzerinde alınacak bazı önlemlerle kapatmak mümkündür.

Çözüm -1

- Switch'lerin IP adresi – MAC adresi eşleşmelerini (ARP tablosu) port bazında tutmalarıdır. (Bu işlem gelişmiş yapıda switch'ler üzerinde gerçekleştirilebilir (VLAN özellikli switchler v.b) . Bu durumda SWİTCH, üzerinden akan ARP paketlerini sürekli olarak denetler. Geçerli veya taklit paketleri bulur. Buna "Dynamic ARP Inspection **(DAI) –Değişken ARP denetimi-**, Dynamic ARP Protection"denir. CİSCO Catalyst 4500 serisi Switch'de bu özellik vardır.
- Switch üzerinde port bazındaki IP adresi – MAC adresi eşleştirmesi yapıldığından, saldırgan bağlı olduğu switch portundan farklı IP adresi – MAC adresi eşleşmelerine sahip olan ARP mesajları gönderemez.
- Bu yöntem DHCP sunuculu sistemlerde uygulanır.
- DAI MAC adresi-IP adresi eşleşmelerini sürekli takip ederek *"Ortadaki Adam"* saldırılarının önlenmesine yardım eder.

Çözüm – 2:

- Bir DHCP sunucusunun bulunmadığı bir ortamda (IP adreslerinin statik olduğu) IP adresi – MAC adresi eşleşmelerinin anahtarlama cihazları üzerinde el ile birer birer yapılması gerekmektedir. Yani DHCP sunucusundan hazır olarak alınan IP adresi – MAC adresi eşleştirmelerinin switch'e el ile girilmesi gerekmektedir. Bunun için anahtarlama cihazları üzerinde ARP erişim kontrol listeleri (ARP access control lists - ARP ACLs) tanımlanır.

Çözüm – 3:

- Saldırı için bir başka çözüm de, anahtarlama cihazının portlarına birim zamanda gelen ARP mesajlarını sınırlamaktır. Bu şekilde, ARP servis dışı bırakma saldırılarının da (ARP DoS) önüne geçilmiş olunur. Bu özellik, sadece Cisco marka anahtarların bazı modellerinde aktif hale getirilebilmektedir.

BMÜ-471 Ağ Güvenliği

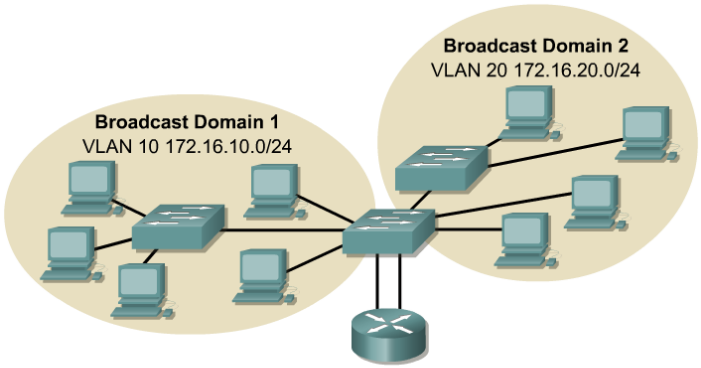
4.Hafta - VLAN

Virtual Local Area Network

Virtual Local Area Network (VLAN)

- VLAN OSI 2. katmanda çalışır (Layer 2). VLAN, bu teknolojiyi destekleyen cihazlar üzerinde mantıksal ağlar oluşturma işlemidir.
- VLAN, yerel alan ağı üzerindeki ağ kullanıcılarının ve kaynaklarının mantıksal olarak gruplandırılması, farklı broadcast domainlere atanması ve ağ cihazları üzerinde farklı portlara atanması ile uygulanır.
- VLAN ölçeklenebilirlik, güvenlik ve ağ yönetimi için yapılandırılır.
- VLAN kullanılan bir ağda, bir VLAN'da bulunan kullanıcılar sadece kendi broadcast domain'ine sahip olacağından, birbirleri ile haberleşebilirler. Oluşturulmuş farklı bir VLAN'da bulunan kullanıcılar ile iletişim kuramazlar. Bu yapılandırma Büyük ağlarda hem ağ trafiğini azaltma, yönetme hem de gurup bilgisayarlar arasındaki erişim güvenliği açısından oldukça önemlidir.
- 2.katmanda önemli bir güvenlik yapılandırması olmakla beraber açıklarıda vardır.

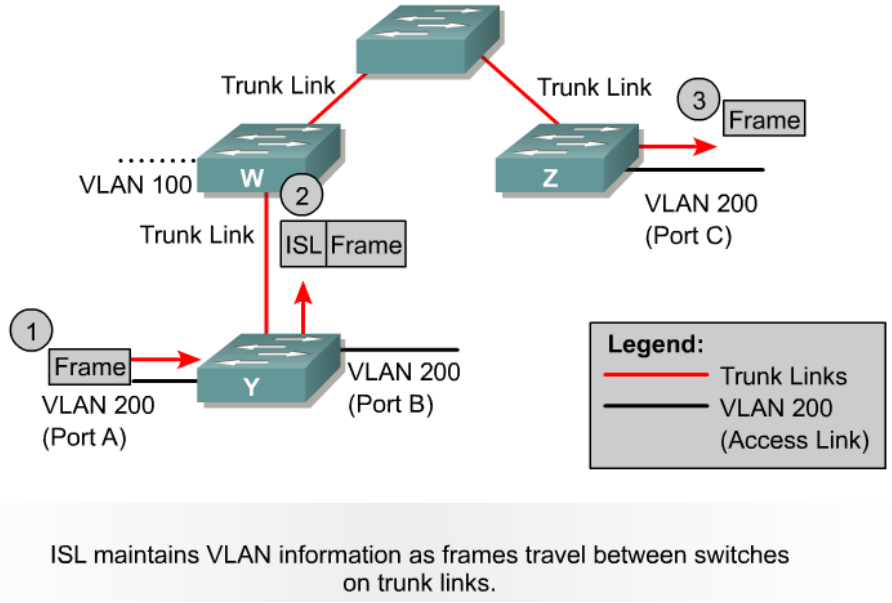
VLAN'lar arasında trafik sadece 3.katman switchleri (Router'lar) ile yönlendirilmelidir



VLANs plus routers limit broadcasts to the domain or origin.

VLAN'lar Farklı veya aynı swithclerin (2.Katman) farklı portlarına bağlı hostlar ile bir broadcast domaini (farklı Subnet'te denebilir- veya mantıksal ağlar) oluşturmasına izin verir.
Farklı VLAN'lere üye olan bilgisayarlar ağ üzerinden birbirlerine erişemezler. Bir VLAN'in ARP isteği diğer VLAN'lere normalde hiçbir şekilde ulaşamaz. Çünkü herbir VLAN farklı bir "broadcast domain"idir.

Access ve Trunk Bağlantıları (Links)



ISL maintains VLAN information as frames travel between switches on trunk links.

ISL: İnterSwitch Link.
ISL , switchler arasındaki trunk linklerinde seyahat eden çerçevelerin bilgilerini tutar.

Cisco switchlerin portları ya "access port" ya da "trunk port" olarak tanımlanabilirler. "access port", bir adet VLAN'e (Native LAN) atanmış port olarak bilinir. "access port"ların, bağlı bulundukları VLAN haricindeki diğer VLAN portlarına erişimi yoktur.
TRUNK Port, switchler arası veya switch-router arası linklerdir. Bu portun üzerinden farklı Vlan paketleri geçebilir.

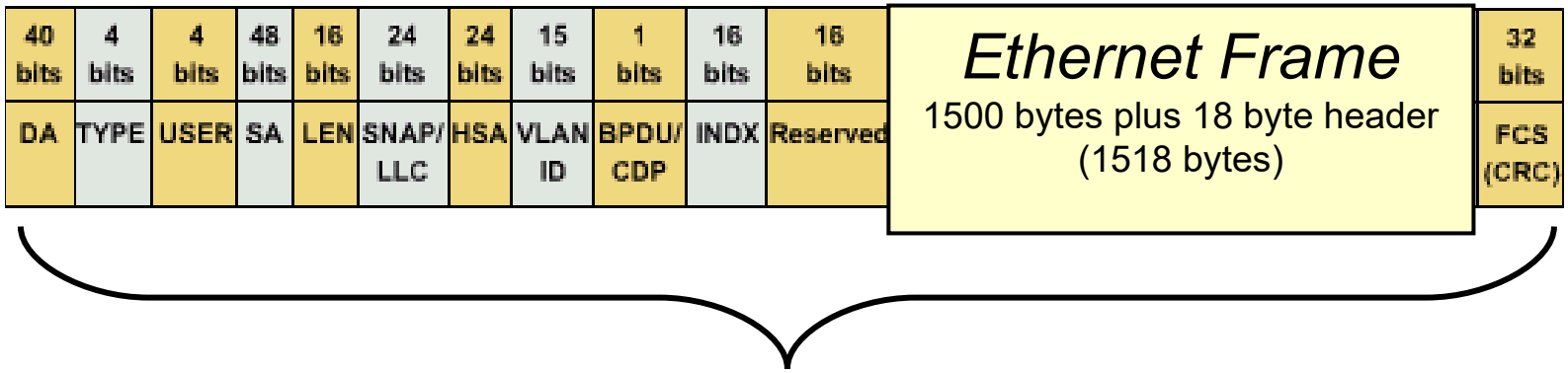
VLAN konfigirasyonu

```
Switch# show running-config
!
interface FastEthernet0/1
 switchport access vlan 50
!
interface FastEthernet0/2
 switchport access vlan 50
!
interface FastEthernet0/3
 switchport access vlan 50
!
interface FastEthernet0/4
 switchport access vlan 50
```

ISL ve IEEE802.1Q

- Anahtarlar arasındaki trafiğin ayırt edilebilmesi için “trunk port”, üzerinden geçen çerçevelere (frame) bir etiket eklenmelidir. Bu etiketleme mekanizması iki türlü yapılır. Bunlar;
- IEEE 802.1q etiketlemesi,
- ISL (InterSwitch Link) etiketlemesi : Sadece Cisco anahtarlarda çalışabilen etiketlemedir.
- Anahtarlar arası VLAN erişiminin sağlanması için anahtarları birbirine bağlayan “trunk port”ların aynı etiketleme türüne sahip olması gereklidir. (Karşılıklı bağlanmış olan “trunk port”ların ya IEEE 802.1q ya da ISL etiketli olması gereklidir.)

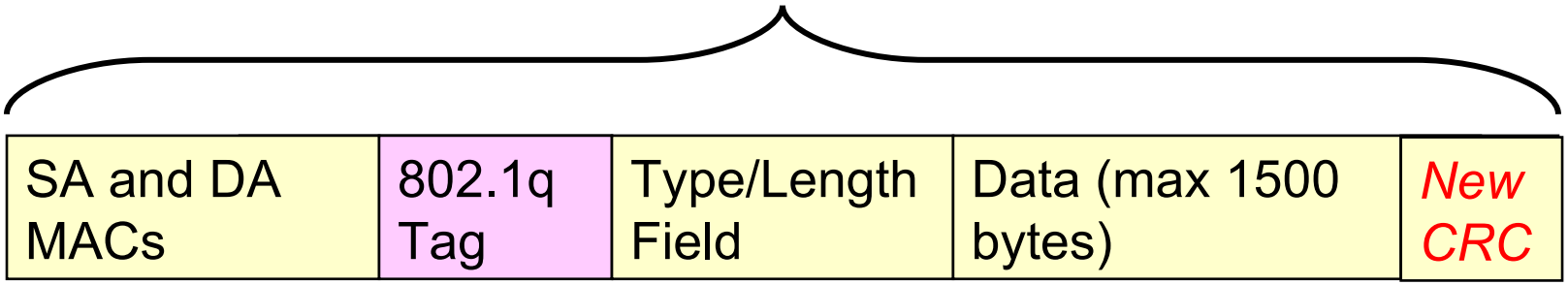
ISL (Frame Encapsulation)



Standart NIC kartları ve ağ cihazları bu büyük çerçeveyi tanımlayamaz. Bir Cisco switch bu çerçeveyi bir erişim Acces link portuna göndermeden önce bu kapsüllemeyi kaldırmalıdır.

802.1q

NIC kartları ve ağ cihazları bu çerçeveyi (1522 bayt) anlayabilir. Bununla birlikte, bir Cisco anahtarı, çerçeveyi bir erişim (acces) bağlantısına göndermeden önce bu kapsüllemeyi kaldırmalıdır.



2-byte TPID — Tag Protocol Identifier

2-byte TCI — Tag Control Info (includes VLAN ID)

Bir portu VLAN TRUNK olarak yapılandırmaya başlamadan önce, portun hangi kapsülleme protokollarını (IDL veya 802.1q) desteklediğini belirlemek gerekir:

```
switch(config-if)# switchport trunk encapsulation ?
```

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode [access | multi | trunk]

Switch(config-if)# switchport trunk encapsulation {isl|
dot1q}

Switch(config-if)# switchport trunk allowed vlan remove
vlan-list
Switch(config-if)# switchport trunk allowed vlan add vlan-
list
```

By default, all VLANS, 1-1005 transported automatically

VLAN Konfigürasyonu

- Switchler üzerinde VLAN'lar oluşturulur.

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name VLAN2
Switch(config-vlan)# exit
Switch(config)# vlan 3
Switch(config-vlan)# name VLAN3
Switch(config-vlan)# exit
Switch(config)# exit
Switch#
```

VLAN Konfigürasyonu

- İlgili portlar/cihazlar bu VLAN'lara üye yapılır.

```
Switch> enable
Switch# configure terminal
Switch(config)#i nt fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# int fastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config-if)# exit
Switch(config)# int fastEthernet 0/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)#
```

VLAN Konfigürasyonu

- Eğer birden çok switch varsa VTP kullanılarak daha etkin PDU paylaşımı sağlanır.

Switch> **enable**
Switch# **vlan database**
Switch(vlan)# **vtp domain MyCompanyArea**
Changing VTP domain name from NULL to MyCompanyArea
Switch(vlan)# **vtp client**
Setting device to VTP CLIENT mode.
Switch(vlan)# **exit**
APPLY completed.
Exiting....
Switch#

VLAN atlama (Hopping) atağı

- Saldırganın, bağlı bulunduğu anahtardan farklı bir anahtar üzerinde kendi VLAN'i haricindeki, normalde erişememesi gereken bir VLAN'e erişmesine *VLAN atlama atağı* denmektedir.

- VLAN atlama atakları ikinci katmanda (Layer 2) gerçekleştirildiği için IP tabanlı (Layer 3) saldırı tespit ya da engelleme sistemleri tarafından yakalanmaları mümkün değildir.

VLAN Hopping Atakları

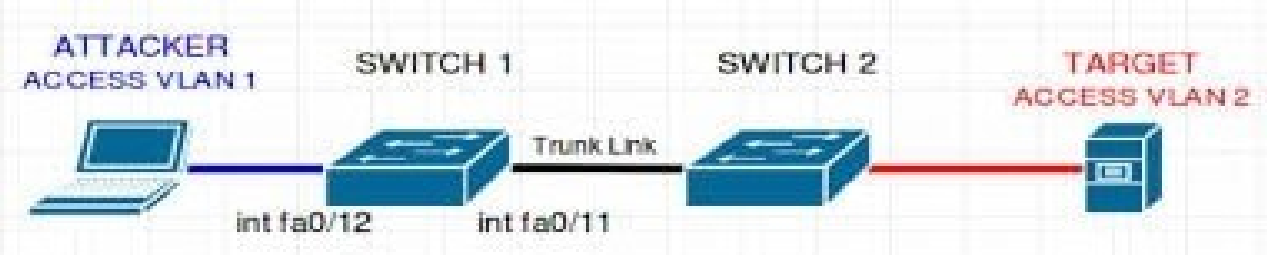
a) Anahtar Sahtekarlığı (Switch Spoofing)

- Bu atak türü, Cisco switchlere yönelik bir ataktır. Cisco anahtarlarının portları ya "access port" ya da "trunk port" olarak tanımlanabilirler.
- "access port", bir adet VLAN'e atanmış port olarak bilinir. "access port"ların, bağlı bulundukları VLAN haricindeki diğer VLAN portlarına erişimi yoktur.
- "trunk port" ise anahtar üzerinde yer alan tüm VLAN'lere üyedir ve switch-switch veya switch-Router bağlantısı ile birçok VLAN bilgisi taşınır.
- Bir portu Trunking mode olarak ayarlamanın ise elle ve otonom olarak Dynamic Trunking Protocol (DTP) olacak şekilde iki farklı konfigürasyon seçeneği mevcuttur.

- Buna göre anahtar kandırma atağının nasıl yapıldığını inceleyelim:

- Cisco switchlerin portları beş modda çalışırlar: “on”, “off”, “desirable”, auto” ve “nonegotiate”. Cisco anahtarların portları ön tanımlı (default) olarak “dynamic desirable” modundadırlar. Bu da şu anlama gelmektedir: Bu portun karşısındaki port “access port” ise port kendisini otomatik olarak “access port” olarak tanımlayacaktır. Karşısındaki portun modu “on”, “auto” ya da “dynamic desirable” ise port kendisini “trunk port” olarak tanımlayacaktır.

Saldırgan, kendi bağlı olduğu switch üzerinde kendisine bakan interface konfigürasyonunun "dynamic desirable", "dynamic auto" veya "trunk mode" olması durumunda, switch gibi davranıp kendi cihazından DTP (Dynamic Desirable Protocol) mesajları oluşturarak TRUNK bir bağlantı kurmuş olacaktır. Yani kendi bilgisayarınında bir switchin trunk portu olduğunu tanıtacak ve dolayısıyla hedeflediği VLAN'lar ile iletişim kurabilecektir..



FastEthernet0/12 için:

```
interface FastEthernet0/12
switchport mode dynamic auto
```

FastEthernet0/12 interface'i karşıdan gelecek olan paketler ile mode seçimine karar verecektir. Bu durumda saldırgan bunu kötüye kullanabilecektir. Saldırgan herhangibir saldırı aracıyla bu porta DTP mesajları göndererek karşıdaki switch ile trunk bağlantı kuracaktır.

b) Çift Etiketleme (Double Tagging)

- Bu saldırının anlaşılabilmesi için “native(yerel) VLAN” ve IEEE 802.1q kavramları önemlidir.
- **Yerel VLAN (Native VLAN):** "Trunk" bağlantı noktasına atanmış VLAN'dır. Bir "Trunk" bağlantı noktası; hem VLAN etiketi olmayan trafiği (untagged traffic) hem de, çok sayıda VLAN tarafından oluşturulan trafiği de (tagged traffic) destekler. "Trunk" bağlantı noktası herhangi bir VLAN'dan gelmeyen trafiği Yerel VLAN'a yönlendirir. Bir cihaz tarafından oluşturulan ve herhangi bir VLAN'dan gelmeyen trafik anahtarlayıcının Yerel VLAN olarak yapılandırılmış olan vlan üzerinden iletilir.

- Normalde anahtar üzerindeki her bir port sadece bir VLAN’e üye yapılabilir. Bir porttan birden fazla VLAN’e iletim için ilgili porta IEEE 802.1q tanımlamasının yapılması gereklidir. Yani TRUNK PORT. IEEE 802.1q tanımı yapılmış olan port, kendisine gelen çerçevenin “MAC adresi” ve “EtherType” alanlarının arasına 32-bitlik bir başka alan (tag-etiket) ekler. IEEE.802.1q portu, sadece etiketlenmiş çerçeveleri iletir. Etiketlenmemiş çerçeveler IEEE 802.1q portundan geçemezler.

- Bunun istisnası “native VLAN”e üye olan çerçevelerdir. IEEE 802.1q portuna gelen ve “native VLAN”e üye olan çerçeveler, herhangi bir etiketlenme yapılmaksızın IEEE 802.1q portu üzerinden karşıdaki anahtara iletilirler.

- Karşılıklı bağlanmış switchler arasında VLAN iletişiminin yapılabilmesi için karşılıklı bağlanmış bu anahtarların IEEE 802.1q portlarının “native VLAN” numaralarının aynı olması gereklidir.

- IEEE 802.1q portuna etiketlenmemiş çerçeve gelirse bu çerçeveler “native VLAN”e üye kabul edilirler. Özetle, IEEE 802.1q tanımı yapılmış olan portlar “native VLAN” için normal bir port gibi davranır.

“native VLAN” özelliği çift etiketlenmiş VLAN atlama saldırılarına açıktır. Şimdi çift etiketleme saldırısının nasıl yapıldığına bakalım:

Herhangi bir tanımlama yapılmadığı takdirde, bir IEEE 802.1q portunun “native VLAN” numarası “1”dir (VLAN 1). Saldırgan, oluşturmuş olduğu çift VLAN etiketli çerçevenin, dış VLAN etiket numarasına “native VLAN”in numarasını verir. İç VLAN etiket numarası olarak da hedef anahtarda yer alan hedef VLAN’in numarasını verir.
örnekle açıklayalım:

Saldırgan, kendisini “native VLAN”e üyeymiş gibi gösteren bir çerçeve oluşturur. Tabii ki bu saldırıyı yapabilmesi için saldırganın, bağlı olduğu anahtarın “native VLAN” numarasını bilmesi gereklidir. Yukarıda da belirtildiği gibi “native VLAN” için herhangi bir tanım yapılmamışsa, VLAN 1 “native VLAN”dir ki “native VLAN” numarası da anahtarlarda genellikle değiştirilmemektedir.

Bu durumda saldırgan kendisinin VLAN 1’de olduğunu belirten bir çerçeve oluşturur. Bu çerçeveye 32-bitlik bir etiket ekler (IEEE 802.1q etiketi). Bu ilk etiketin içindeki VLAN değerine de (VID) “1” verir.

Bundan sonra saldırgan, çerçeveye ikinci bir 32-bitlik etiket daha ekler. Bu etiketin içine de saldırıyı yapacağı VLAN’in numarasını yazar. Bu şekilde saldırgan çift etiketli bir çerçeve oluşturmuş olur. (Bu şekilde özel çerçevelerin (frame) oluşturulabildiği programlara internet üzerinden ulaşmak zor değildir.)

Aşağıdaki örnekte IEEE 802.1q portlarının “native VLAN” numarası “1” olarak kabul edilmiştir. Saldıracağımız VLAN’in numarasının da 61 dir. Bu durumda, çift VLAN etiketli çerçevenin dış VLAN etiketi ”1”, iç VLAN etiketi de “61” olarak belirlenir.

Saldırganın hedefindeki VLAN, “61” numaralı VLAN’e bağlı olan bilgisayarlardır. Saldırgan, göndermiş olduğu çerçeveye çift etiket eklemiştir. “1” numaralı anahtarın IEEE 802.1q portuna gelen çerçevedeki dış etiket “1” numaralı “native VLAN”e ait olduğundan anahtar “1” numaralı etiketi çıkarır ve çerçeveyi karşıdaki “2” numaralı anahtara gönderir. “2” numaralı anahtarın IEEE 802.1q portu da kendisine gelen bu çerçevenin “61” numaralı VLAN etiketini okuyarak çerçeveyi “61” numaralı VLAN’e ait olan portlara gönderir. Bu şekilde saldırgan “2” numaralı anahtarda yer alan “61” numaralı VLAN’e erişmiş olur. Saldırgan, “61” numarasını değiştirmek suretiyle “2” numaralı anahtarda tanımlanmış olan herhangi bir VLAN’e erişebilecektir. Saldırganın yapması gereken tek şey, iç VLAN etiket numarasının yerine erişmek istediği VLAN numarasını yazmaktır.

Önlem

- Anahtar kandırma (switch spoofing) atağını engellemek için anahtarın portlarından DTP (DynamicTrunking Port) özelliğini kaldırmak gerekir.
- IEEE 802.1q portuna ihtiyacımız olduğu takdirde bunun manuel olarak yapılması tavsiye edilir. Aşağıdaki komut satırı girilmek suretiyle anahtarın portlarından DTP kaldırılmış olur:

ANAHTAR(config)# interface range FastEthernet 0/1 – 24
ANAHTAR(config-if)# switchport mode access

- Çift etiketleme atağından korunmak için de aşağıdaki maddeler tavsiye edilir:

1. “native VLAN”i kullanıcılar için kullanılmaması,
2. “default VLAN” numarasına “1”den farklı bir değer verin ve bu VLAN’i kullanıcılar için kullanılmaması,
3. Kullanılmayan portları kapatın ve bu portları “default VLAN” haricinde başka bir VLAN’e dahil edilmesi

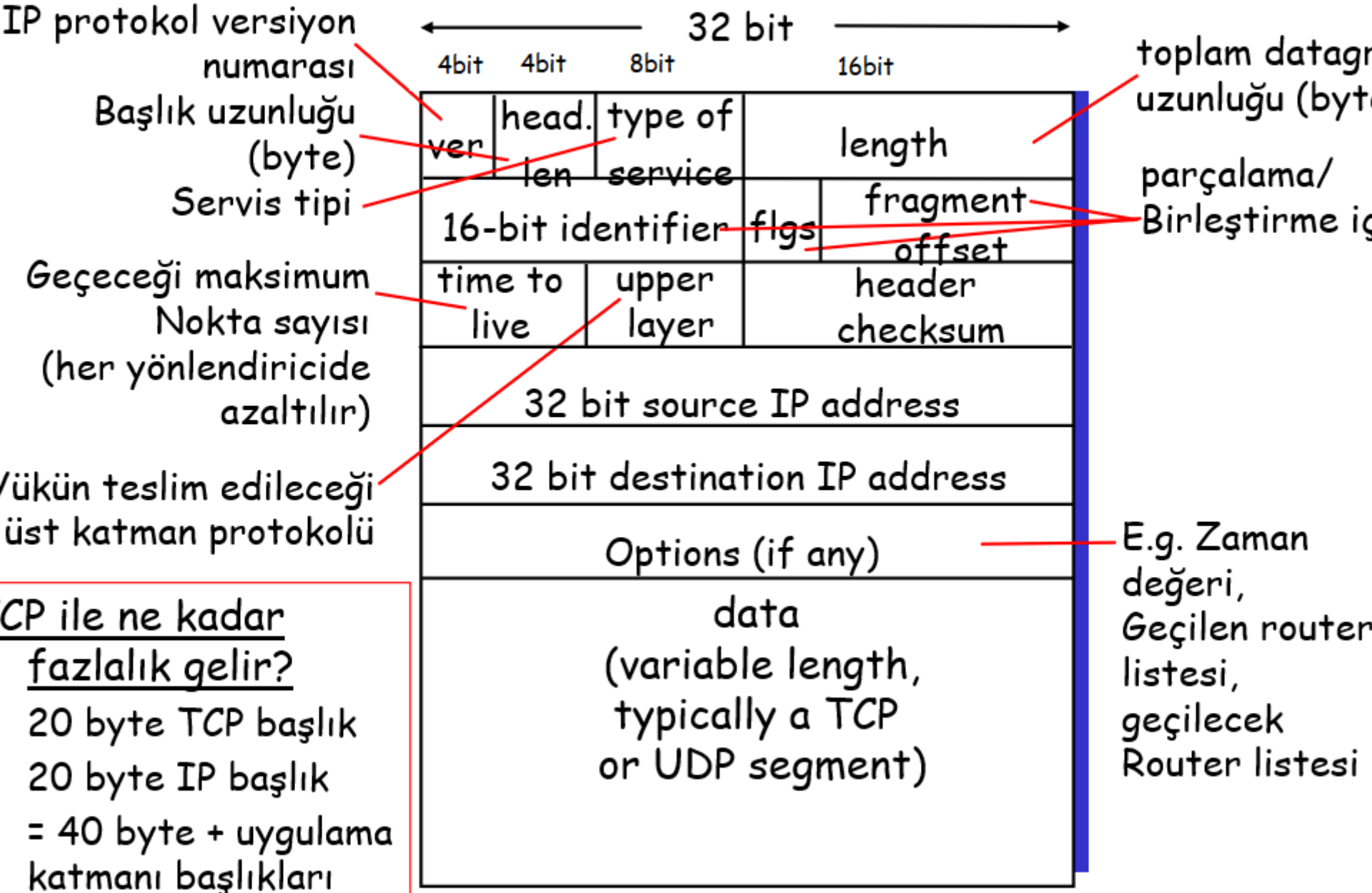
BMÜ-457 Ağ Güvenliği

5.Hafta
Network Katmanı (3.Katman) Atakları - Güvenliği - 1

Ağ katmanı - IP

- Farklı Fiziksel segmentlerdeki (LAN- veya farklı ağ) bilgisayarlar arasındaki paketleri taşımak için yapılması gerekenleri tarif eder.
- Bunun için kullanılan temel işlemler;
  - Routing (Yönlendirme): Rota keşfi ve mantıksal adreslemeye göre ağlar arası seyahat.
  - Düşük katmanlardaki adres keşfi işlemi : (Alt katman adresleri arama)
  - Error Messages (ICMP) (Hata mesajlaşma)

IP datagram formatı



TCP ile ne kadar fazlalık gelir?

20 byte TCP başlık

20 byte IP başlık

= 40 byte + uygulama katmanı başlıkları

IP Router'lar

- Router'lar ağ katmanında çalışırlar ve ağ adreslerine göre ağdaki paketleri yönlendirirler.
- Router'lar IP datagramlarının yerine teslimini direkt veya dolaylı olarak desteklerler.
- Hedefe varabilecek olası yolları kullanmak için Yönlendirme tablolarını kullanırlar.
- Bir datagram için 3 olası durum sözkonusudur.
  - Doğrudan hedef Host'a gönderilme.
  - Bilinen hedef yolundaki bir sonraki router'a gönderilme.
  - Default Router'a gönderilme
- IP Routerlar, katman 3'te çalışırlar.

Router'ların GÜVENLİĞİ

1-Fiziksel Güvenlik:

Yönlendiriciler için ayrı bir oda ayırılamıyorsa en azından kilitli dolaplar (kabinet) içine koyulmalıdır. Bu odanın enerjisi hiç kesilmemelidir

2.Yönlendiriciye Erişim Hakları

Yönlendiriciye kimlerin erişeceğinin bir politikayla belirlenmesi ve erişimlerin loglanması gerekmektedir. Temelde yönlendiricilere, **kullanıcı (user)** ve **yönetici (enable)** olarak iki çeşit erişim hakkı vardır. Kullanıcı modunda sadece kontroller yapılabilirken, yönetici modda ek olarak cihaz konfigürasyonu da yapılabilmektedir.

3.Şifrelerin Güvenliği

Cisco yönlendiricilerde kullanıcı adı ve parolasının konfigürasyon dosyasında gözükmemesi için *"service password-encription" komutu kullanılmalı. Zayıf şifreleme algoritması kullanan "enable password" kaldırılmalı, MD5-tabanlı algoritmayla şifreyi koruyan "enable secret"* komutu kullanılmalıdır.

Router güvenliği-3

4.Erişim Protokollerinin Güvenliği

Routerlara fiziksel erişim konsol portundan yapılmaktadır. Bunun için fizikselgüvenliğin sağlanması gerekmektedir.

Diğer erişim yöntemleri olan HTTP, Telnet, SSH,TFTP, ve FTP kullanıldığında TCP/IP protokolünün zayıflıklarına karşı önlem alınması gerekmektedir. Alınması gereken önlemler aşağıdaki gibidir.

a) Belirli IP'lerin Cihaza Erişimine İzin Vermek:

Cihazlara sadece belirli IP adreslerinin ulaşmasına izin verilmelidir. Bu da erişim listesi (access-list) yazılarak sağlanır. Örneğin Cisco IOS'de sadece 200.100.17.2 ve 200.100.17.3 IP'lerin erişimine izin verilmesi ve diğer ip'lerin engellenmesi ve bu erişimlerin kaydının tutulması aşağıdaki erişim listesi ile sağlanmaktadır.

access-list 7 permit 200.100.17.2
access-list 7 permit 200.100.17.3
access-list 7 deny any log

R.Güvenliği -4

HTTP Erişimi:
HTTP protokolü ile web arayüzünden erişim, cihaza interaktif bağlantı demektir. Yönetilebilir cihazlarının birçoğunun üzerinde web sunucusu çalışır. Bu da 80 nolu portta bir web sunucunun kurulu beklediğini gösterir.

Web üzerinden yönetim gerekiyorsa web sunucusu sadece sistem yöneticisinin bileceği başka bir port üzerinden, örneğin *"ip http server port 500"* komutuyla 500 nolu portta çalıştırılabilecek şekilde ayarlanmalıdır.

R.Güvenliği-6

5.Gereksiz Servisleri Kapatmak

Yönlendiricide kullanılmayan servisler kapatılmalıdır. Örneğin kullanılmayan ve güvenlik açığı oluşturabilecek TCP/UDP services echo, chargen ve discard kapatılmalıdır:

no service tcp-small-servers
no service udp-small-servers

Bu cihaza bağlı kişiler hakkında saldırgana bilgiler sağlayabilecek "finger" servisi de kapatılmalıdır:

no service finger

Daha önceden de belirtildiği üzere yönlendiricide web sunucusu da çalıştırılmamalıdır:

no ip http server

Ağı R ile korumak-2

Bu bölümde yönlendirici ile ağdaki bilgisayarlara gelebilecek saldırıların engellenmesi için bazı ipuçları verilecektir.

1. Riskli portları kapatmak:

İnternet üzerindeki servisler, kullanıcılara hizmet götürebilmek için bazı sanal port numaraları kullanırlar (örn: http için 80 numaralı port kullanılmaktadır). Saldırganlar veya kötü yazılımlar servislerin açıklarını kullanarak hizmet verilen port numarası üzerinden bilgisayar ağına sızabilirler.

Bunu önlemenin bir yolu riskli portları yönlendirici ile kısıtlamaktır. Riskli portların listesi [http://www.nsa.gov/snac/cisco/guides/cis-2.pdf] adresteki referansının 38 ve 39 sayfalarında listelenmiştir. Aşağıdaki örnekte 445 nolu UDP portu ile finger servisi bloklanmaktadır:

access-list 101 deny udp any any eq 445
access-list 101 deny tcp any any eq finger
access-list 101 permit ip any any

Ağı R ile korumak-3

2.Bazı saldırı tekniklerine karşı önlemler

IP spoofing : Kötü niyeli kişi hattı dinler giden paketlerin kaynak ve hedef adresini alır. Hedef adresini kendi ip'si yaparak kaynak adrese cevap verir. Böylece erişim listesine takılmadan bilgisayar ağına sızmış olur.

Bunu önlemenin yolu, yönlendiricinin kaynak adresi hedef makinaya varmadan kimseye göstermemesidir. Bu işlem Cisco cihazlarda "*no ip source-route" komutuyla yapılabilmektedir* .

Routing Protokole olan saldırılar: Saldırgan yönlendiricinin routingprotokolünü bozmadan yollanan paketlerin bir kopyasının kendine de yollanmasını sağlayabilir veya protokolleri kaldırarak yönlendiricinin diğer yönlendiricilerle haberleşmesini kesebilir. Haberleşmenin yok olması, yönlendiricinin aldığı paketleri nereye göndereceğini bilmemesi ve servis dışı kalması(DoS) saldırısıdır. Bunu önlemenin yolu ise gönderilen ve alınan routing protokolu paketlerini filitrelemektir. Örneğin IGRP routing protokolünü filtrelemek için yazılmış ACL aşağıda verilmiştir.

router eigrp
network 200.100.17.0
distribute list 20 out ethernet 0
distance 255
distance 90 200.100.17.0 0.0.0.255
access-list 20 permit 200.100.17.0 0.0.0.255

Ağı R ile korumak-4

Çıkış (Egress) ve Giriş (Ingress) Erişim Listeleri:
Dış ağdan iç ağa gelen paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne *giriş (ingress) filtreleme denmektedir. Bu kontrolde gelen paketlerdeki ip'lerde internet ortamında* kullanılmayan (rezerve edilmiş) adresler bulunduğunda bu paketler kabul edilmeyecektir.
Ağ adresimiz 200.100.17.0/24 ise, dış dünyadan böyle bir IP aralığına ait bir paket gelmemesi gerekmektedir. O zaman ingress kısıtlamaları aşagıdaki gibi olacaktır:

access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 deny ip 200.100.17.0 0.0.0.255 any
access-list 101 permit ip any an

Ağdan dış ağa giden paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne *çıkış (egress) filtreleme denmektedir. Kendi ağ ip adresi aralığında olmayıp da internete çıkmak isteyen* ip'ler kısıtlanmalıdır.

access-list 102 permit ip 200.100.17.0 0.0.0.255 any
access-list 102 deny ip any any

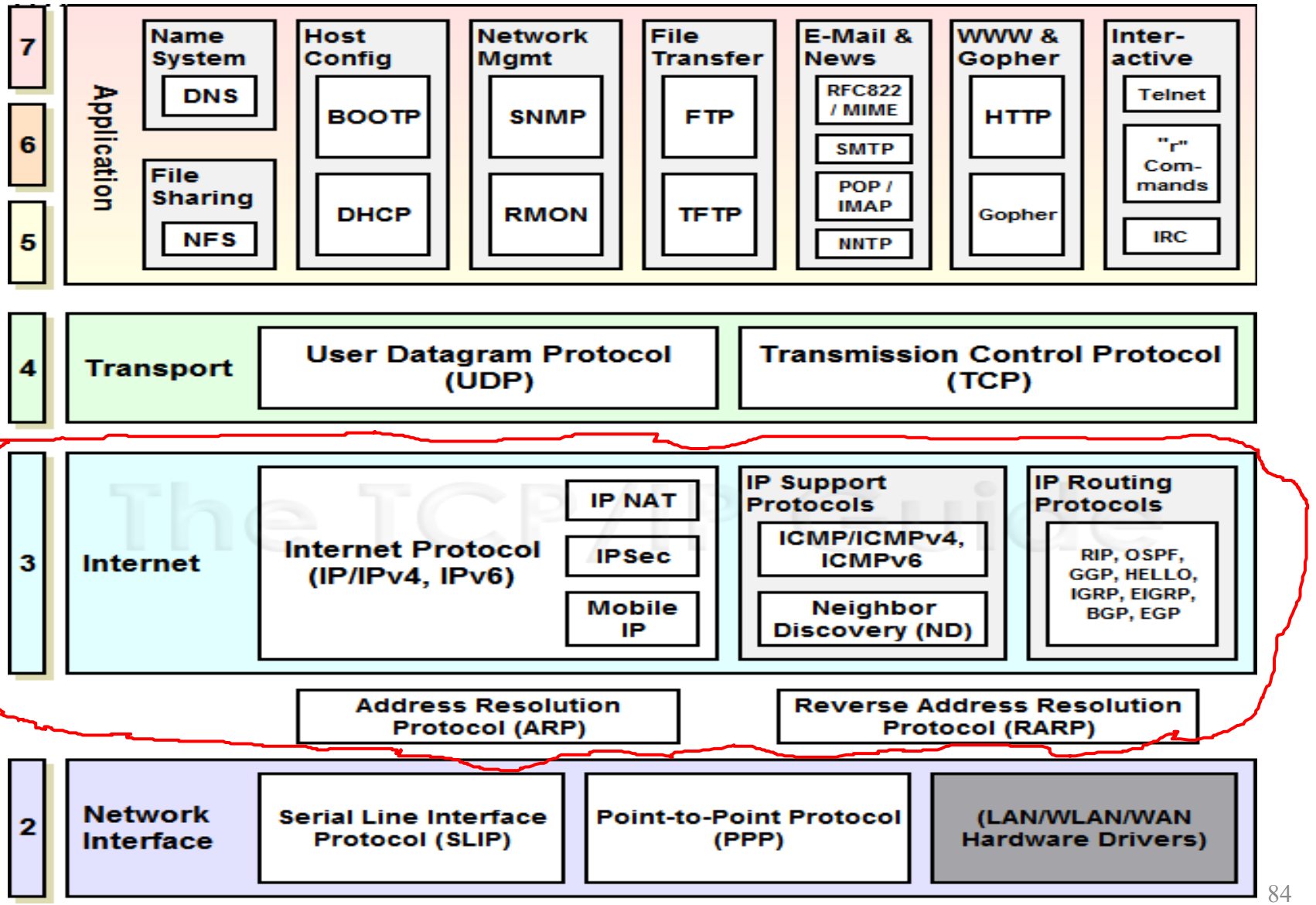
BMÜ-457 Ağ Güvenliği

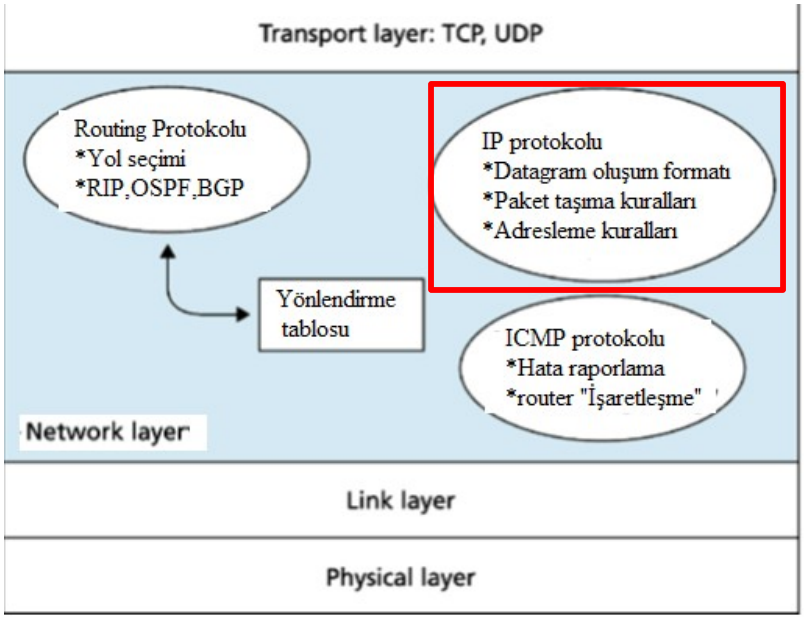
6-7.Hafta
Network Katmanı (3.Katman) Atakları - Güvenliği -2

Ağ katmanı - IP

- Farklı Fiziksel segmentlerdeki (LAN- veya farklı ağ) bilgisayarlar arasındaki paketleri taşımak için yapılması gerekenleri tarif eder.
- Bunun için kullanılan temel işlemler;
  - Routing (Yönlendirme): Rota keşfi ve mantıksal adreslemeye göre ağlar arası seyahat.
  - Düşük katmanlardaki adres keşfi işlemi : (Alt katman adresleri arama)
  - Error Messages (ICMP) (Hata mesajlaşma)

TCP/IP protokol kümesi





IP protokolu Saldırıları

*** IP spoofing:** Paketin kaynak adres kısmının olması gerekenden farklı bir IP adresi ile değiştirilmesidir.

1-ARP spoofing (Paketin kaynak adres kısmındaki sahte IP)

2-Source Routing (Kaynak Rotalama, kaynak adres kısmı sahte IP)

*** IP Fragmantasyon Atağı:**

*** Trafik arttırma atağı:** IP broadcast hedef'e müsaade eder. DOS..

IP Protokolu zayıflıkları

1.Gizlilik: Bir paketin bir noktadan çıkıp karşı noktaya iletildiği yol boyunca gizlenmemesi sebebi ile paketin içeriği yol boyunca, izlenebilir ve okunabilir.

2.Paket doğrulama yoktur: Bir paketin kaynak adresi değiştirilmiş olabilir. Ipv.4 paketinde bunun doğru bir kaynak adresi olup olmadığının doğrulaması yoktur. Genelde Spoof (Hırsızlık) ismi verilen saldırıların temeli bu zayıflıktır.

3.İçerik bütünlüğü korunmaz: Paketin başlığının ve içeriğinin yolda değiştirilmediğini garanti eden bir tedbir yoktur.

4.Paketlerin parçalanması ve birleştirilmesi süreci: Bu süreçte bir doğrulama ve kontrol mekanizması yoktur

IP Spoofing (Yanıltma-Aldatma)

- Internet veya ağa bağlı sisteminizle başka bir sisteme bağlanacaksınız, fakat bu bağlantının sizin tarafınızdan yapıldığını gizlemek istiyorsunuz. Bunun için bağlantı sırasında kimliğinizi (ki TCP/IP protokollerinde kimliğiniz IP adresinizdir), yanlış gösteriyorsunuz. **Bu IP spoofing işlemidir**.

- Bu saldırıyla, saldırgan, kendi IP paketlerinin sahtekarlığını yaparak (nemesis v.b gibi programlar ile) diğer paketlerin arasındaki kendi paketinin kaynak IP alanını değiştirir.
- Saldırgan, paketin kaynak adresi olarak dahili veya güvenilir bir IP adresi koyar. Böylelikle Erişim kontrol cihazının, IP adresini güvenilir olarak görmesini ve paketi geçirmesini sağlayabilir..
- Kaynak değiştirildiğinden, sahte pakete karşılık gelen cevaplar saldırganın makinesine gidemez. Spoof edilen makinaya gider.

- Saldırganın bu cevabı kendi makinasına alabilmesi için kullandığı önemli teknik "Kaynak yönlendirme-Source routing"'dir.

  - IP spoofing (sahtekarlığı) için iki genel teknik kullanılır:

    * Güvenilir IP adresleri aralığında olan bir IP adresi kullanır.
    * Güvenilen yetkili bir dış IP adresi kullanır.

  IP spoofing kolay başarılacak bir saldırıdır. Çünkü;

    *Yönlendiriciler yalnızca Hedef adreslerine bakar.
    * Yalnızca Kaynak adreslerine göre kimlik doğrulama.
    *IP başlık alanındaki kaynak adres alanını değiştirmek kolaydır.

Spoofing Atakları

1- Yerel spoofing (Non blind spoofing): Saldırgan ve mağdur (victim-kurban) aynı alt ağdadır.

Saldırgan, bir saldırı başlatmak için gerekli temel bilgi parçalarını bulmak amacıyla trafik koklama (sniffing - izleyici) ile işe başlar. Alt ağdaki bir normal kullanıcının gönderilerine müdahale etmek için kullanılır. Bu tür bir sahtekarlık tehdidi oturumun ele geçirilmesi ve bir saldırgan bağlantıyı kurmak için tüm kimlik doğrulama önlemlerini atlayabilir. Bu, kurulan bir bağlantının DataStream'ini bozarak, ardından doğru sıraya ve saldırı numaralarıyla onay numaralarına dayanarak yeniden kurarak gerçekleştirilir, normal bir TCP oturmunu resetleyebilir.

2- Blind spoofing: Saldırgan ile mağdur aynı altağ'da değildir. Daha karmaşık ve gelişmiş saldırıdır. Saldırının başarılması için gerekli bilgi miktarı mevcut değildir. Anahtar parametreleri tahmin edilmelidir. Modern işletim sistemleri bu şekildeki saldırıları başlatmayı zor hale getirmek için, oldukça rastgele sıra numaraları kullanır.

3- Man in the Middle: Ortadaki adam saldırısı. Buna bağlantı hırsızlığıda denir. Bu saldırılarda, kötü niyetli bir taraf, iletişim akışını kontrol etmek ve asıl katılımcılardan birinin gönderdiği bilgileri bilgisi olmadan elemek veya değiştirmek için iki ev sahibi arasında meşru bir iletişim kurar.

4. DOS Saldırısı: Saldırıyı gerçekleştiren saldırganlar, DoS'un izlenmesini ve durdurulmasını mümkün olduğunca zorlaştırmak için kaynak IP adreslerini taklit eder. Birden fazla tehlike altındaki ana bilgisayar saldırıya katılırken, tüm gönderilen sahtekarlık trafiği, trafiği hızla engellemek için çok zordur.

IP sahtekarlığı ayrıca, IP adreslerine dayalı kimlik doğrulama gibi ağ güvenlik önlemlerini yenmek için kullanılan bir saldırı yöntemi olabilir. Bu tür bir saldırı, makineler arasında güven ilişkilerinin olduğu yerlerde en etkilidir.Örneğin, bazı şirket ağlarında,, iç ağdaki başka bir makineden bağlanması şartıyla kullanıcı adı veya şifre olmadan giriş yapabilir (ve çoktan oturum açmış olması gerekir). . Bir saldırgan, güvenilir bir makineden yapılan bir sahtekarlığa sahte olarak, hedef makineye kimlik doğrulaması yapmadan erişebilir.

IP spoofing'in anlaşılması ve önleme

Paketleri wireshark v.b gibi ağ izleme yazılımı kullanarak izlerseniz;

- hem kaynak hem de hedef IP adresinin lokal IP olduğu bir dış ağdan gelen paket, IP sahtekarlığının bir göstergesidir.
- Kullanılan bilgisayardaki trafik loglarının incelenmesiyle d tespit mümkün.

- IP sahtekarlığı sorununu önlemenin en iyi yöntemi, dış ağdan (giriş filtresi olarak da bilinir) gelen paketlerin, iç ağınızdaki bir kaynak adrese sahipse filitrelenmesidir (Router veya Gateway tarafından). Aynı şekilde; iç ağdankaynaklanan bir kaynak IP sahtekarlığı saldırısını önlemek için iç ağınızdan farklı bir kaynak adresine sahip giden paketleri filtrelemelisiniz. Dikkat!!! Bu işlemlerin yapılabileceği bir router veya firewall'a sahip olmalısınız.
- Ağınızda IP sahtekarlığının ortaya çıkmasını önlemek için, bazı yaygın uygulamalar şunlardır:

1- Kaynak adres onayını kullanmaktan kaçının. Sistem genelinde kriptografik kimlik doğrulama uygulayın.

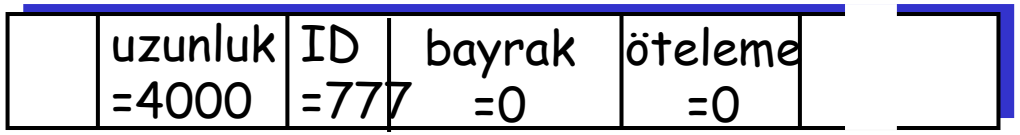
2- Ağınızı, yerel bir adresten kaynaklandığı iddia edilen ağdan gelen paketleri reddetmek üzere yapılandırın.

3- Kenar yönlendiricilere giriş ve çıkış filtreleme uygulamak ve i özel IP adreslerini engelleyen bir ACL (erişim kontrol listesi) uygulayın. Güvenilir ana bilgisayarlardan dış bağlantılara izin veriyorsanız, yönlendiricideki şifreleme oturumlarını etkinleştirin.

IP Datagram Parçalama/Birleştirme

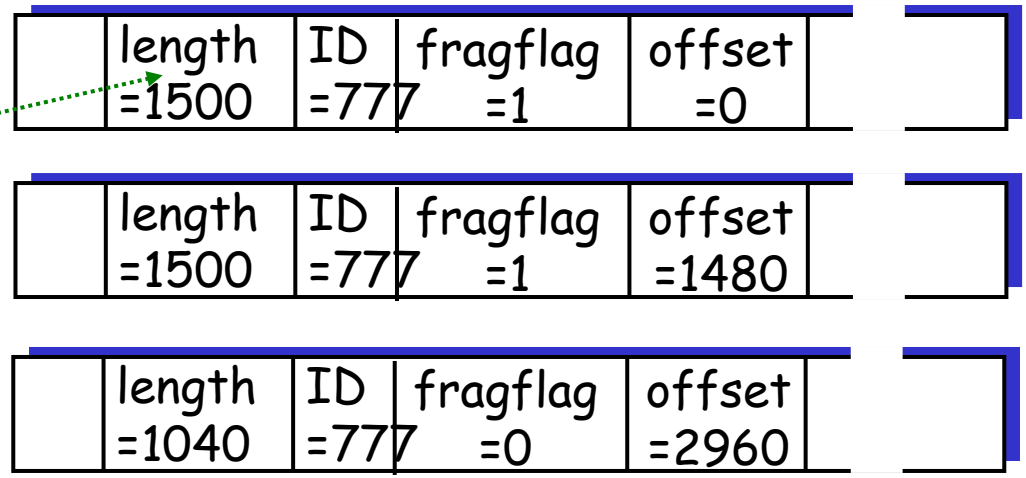
Örnek

- 4000 byte datagram
- MTU = 1500 bytes



Büyük bir datagram birkaç küçük datagrama dönüşür

Veri alanında 1480 bytes



ICMP ?

Her IP paketi ?

- ***Reassembly (*** Tekrar Birleştirilme İşlemleri): IP protokolü belirtimindeki bazı belirsizlikler nedeniyle, özel durumlarda farklı parçalama işlemleri meydana gelebilir ve bu parçaların yeniden birleştirilmesi gerekir. Bu özel parçalama işlemleri;
- ***Fragment retransmission (parçaların yeniden iletilmesi),***
- **Fragment overlays** (parçaların üstüste gelmesi - bindirmeler)
- **Fragments with non-neighbouring offsets**.(Komşu olmayan ofsetli parçalar.)
- Eğer ağı koruyan cihazlardaki parçalar ile hedef hosttakiler farklılıklar gösterir ise; bu durum tutarsızlıklara yola açabilir.
- Dolayısıyla ***insertion*** ve ***evasion*** atakaları yapılabilir.

- **Bu birleştirme sürecindeki olabilecek ataklar;**
- **Time out (Zaman aşımı) :** Parçalanmış paket; yalnızca tüm parçalarının parçalanma zaman aşımı süresi içinde alınmış ise yeniden birleştirilir.
- *Hedef host ve IDS'de farklı zaman aşımı uzunluklarının kullanılması, saldırgana evasion atak gerçekleştirmesine izin verebilir.*
- **TCP header division:** TCP oturumunu izleyip ve parçalanmış paketleri yeniden birleştirmeyi başaramayan IDS'ler, saldırgan tarafından oluşturulmuş daha küçük fragmentleri atlayabilirler. Bunlar TCP başlıkları ikiye üçe bölünmüş fragmentler olabilir.
- *Bu şekilde oluşmuş her bir bağımsız fragment, imzayla uyuşmaz dolayısıyla atak sayılmaz.*

Fragmentation Atakları

- Parçalanmış paketlerin üst üste çakışması (Overlay), saldırganlara IDS, Firewall ve Routerlarda eski paketlerin kaydırılması imkanını sunar.
- Bir routerdan, windows temelli bir sisteme paket gönderildiğinde;
- Eğer alınan paket duplike bir paket ise;
  - Router (veya IDS veya Firewall) en son gönderilen fragmenti tercih eder.
  - Windows orijinal (ilk gönderileni) tercih eder.

Fragmentation Attacks (cont.)

Windows and router accepts #1 and #2

Attacker modifies #2
And transmits #2 and #3

Windows keeps

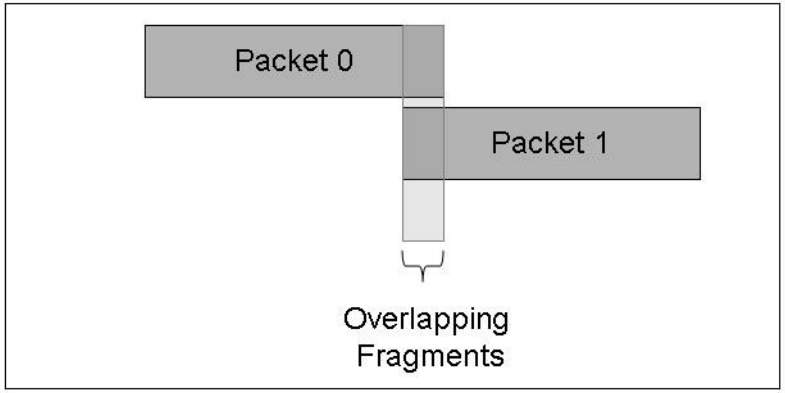
Router keeps

Same size, same offset

Teardrop Saldırıları

- Teardrop, targa, NewTear, Nestea Bonk, Boink, TearDrop2, ve SynDrop gibi bazı saldırı araçları, IP atakları için açıklara sahip makinaları çökertebilirler.
- Teardrop atağı IP paketlerinin tekrar birleştirilmesindeki zayıflıktan yararlanır. Mesaj, ağlar arasında iletilirken genellikle daha küçük parçalar ayrılır. Herbir parça orjinal paket gibi görünür. Fakat offset alanları farklıdır. Teardrop programı bir dizi IP paket parçaları oluşturur. Bu parçalar örtüşen offset alanlarına sahiptir. Bu parçacıklar varış noktasında tekrar birleştirildiklerinde bazı sistemler çökebilir, durabilir veya kapanıp açılabilir. Teardrop saldırısı bir DOS saldırısıdır.
- Overlapping, over-sized, payload paketler gönderilerek sistem bozulur.

Figure 4.14 The Teardrop Attack

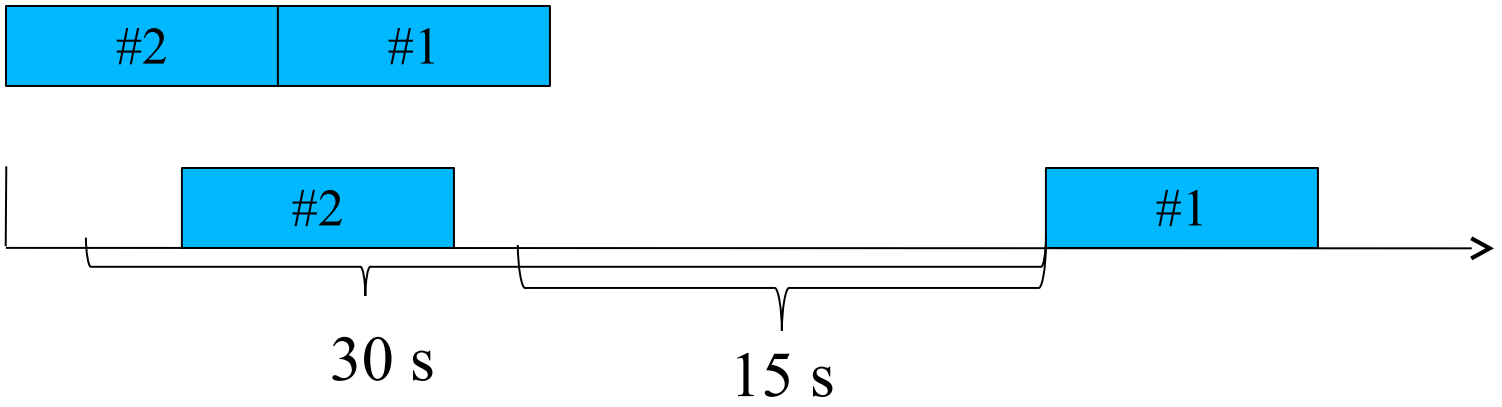


Ping of Death Atağı

- Ping of Death, IP paketlerine gömülü olarak ICMP ile gönderilen “echo request” mesajları ile yapılır. Bu mesajlar 65.535 bayt’tan daha büyük mesajlar halinde sürekli olarak gönerilirse Buffer kapasitesi küçük olan makinalarda buffer taşmasına sebep olarak makinanın çökmesine sebep olur. Ping of death bir DoS atağı çeşididir.

Evasion Attack (Atlatma Atakları)

- Bir saldırgan ilk fragmenti, timeout'u 15s olan IDS'ye ve timeout'u 30s olan hedef sisteme gönderir.
- Saldırgan 15s ile 30 s arasında bir zamanda ikinci fragmenti gönderir.
- IDS 2.fragmenti iptal eder. Çünkü timeout'u 15 s'den büyüktür. Fakat hedef sistem bu fragmenti kabul eder. Oysa bunun içinde bir atak olma ihtimali vardır.
- Böylece IDS atağı kayıt edemez. IDS atlatılmış olur.



Çok bilinen ataklardan bazıları

Time to live field attacks : IP başlığının TTL alanı bir paketin düşürülmeden önce, yönlendirildiği rota üzerinde kaç atlama yapabileceğini ifade ediyordu. Her yönlendirici kendisine gelen paketi yönlendirdiğinde TTL alanındaki değeri bir eksiltiyordu.

- Buna göre , ağ yapısı (topolojisi) hakkında önceden bilgi sahibi olan saldırganlar, paketleri öyle ustalıkla düzenleyebilir ki paketler, ağdaki IDS'ler tarafından düşürülmeden önce (IDS tarafından TTL'den dolayı) hedef hosta normal (TTL değeri 0'lanmadan) gibi ulaşır.

Maximum transmission unit (MTU) : Saldirgan hedef host ile kendisinin kullandığı en düşük MTU değerini, "yol MTU Keşfi" olarak adlandırılan bir teknik ile öğrenebilir.

- Eğer bu minimum MTU değeri IDS ile hedef host arasındaki bağlantıda geçerli ise; saldırgan b u minimum MTU değerinden daha büyük bir boyutlu paket yaratıp "Dont Fragment " bayrağını 1 yapar. Böylece bu paketler IDS tarafından kabul edilir. Fakat daha düşük MTU'lu ağın başındaki router TARAFINDAN (hedef bilgisayar bu Router'ın arkasındaki ağdadır) tarafından reddedilir.
- Bu bir **"IDS insertion"** atağıdır. Böylece, IDS bu paket gurubu için imza analizi yapamaz.

IP checksum verification : IP checsum doğrulaması yapmayan bir IDS sistemi (performans kaybı olmasın diye genlede yapmazlar), insertion ataklarına karşı duyarlıdır. Çünkü bu sistemler hedef host'un reddettiği paketleri kabul edip işleyebilirler.

- IP checksum doğrulama, parçalanma (fragmentasyon)) veya taşıma katmanı saldırıları ile birlikte kullanılır.

BMÜ-457 Ağ Güvenliği

6-7.Hafta
Network Katmanı (3.Katman) Atakları - Güvenliği -2.b

YÖNLENDİRME Protokollarına ATAKLAR (7.Hafta Başlangıcı)

- **Routerların (Yönlendiricilerin) görevlerini tekrar hatırlarsak;**
- **Yerel ağdan gelen paketleri filtrelemek :** Paket filtreleme, network adresi (IP), servisi ve protokolüne göre bilgi transferini kontrol etmektir. Yönlendirici bu kontrolleri ACL'ler (Access-Control List –Erişim Listesi) yardımı ile sağlar. ACL'ler kendisine gelen verinin kaynak, hedef ip adreslerine, bilginin gideceği port adresine veya kullanılmak istenen protokole göre kısıtlamalar yapabilmektedir.
- **Paketlerin nereye gideceğine karar vermek:** Yönlendirici, kendine bağlı olan bilgisayarların network adreslerini tuttuğu gibi, kendisine bağlı veya kullanılan protokole göre bağımsız yönlendiricilerin network adreslerini de routing tablolarında tutmaktadır. Yönlendirici kendisine gelen paketlerin nereye gideceğini öğrendikten sonra bu adresi routing tablolarıyla karşılaştırarak hangi port'undan yollayacağına karar vermektedir.

- Böylece ROUTER ,yerel ağları birbirine bağladığı gibi kurumun WAN'a bağlantı noktasını da oluşturmakta ve internet erişimini de sağlamaktadır.

IP Datagramların Yönlendirilmesi

- Farklı ağlar üzerindeki bilgisayarların haberleşmesi için ağlar arasında datagramların yönlendirilmesi gerekir.
- Router'larda en az iki adet farklı ağa bağlanmak için iki ağ donanım arabirimi bulunmalıdır.
- Routerlar datagramları yönlendirebilmek için hafızalarında *IP Datagram yönlendirme tabloları* bulundurmalıdırlar. Bu tablolarda hedef ağa ulaşabilmek için uygun yönlendiricilerin bilgileri bulunur. Yönlendirme tablosu iki şekilde oluşturulabilir.

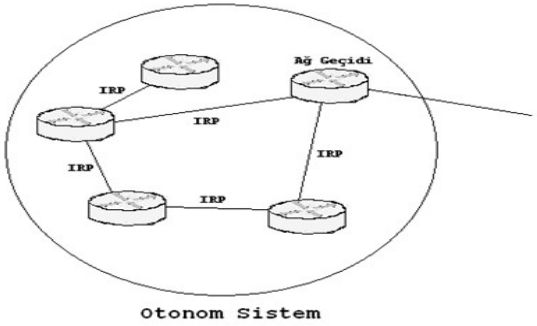
1-Dinamik yapılandırma: Routarlar bünyelerindeki yönlendirme tablo algoritmalarını çalıştırarak, komşularının durumuna göre en uygun ve hızlı yolları belirleyip tablolarını oluşturur ve güncellerler.

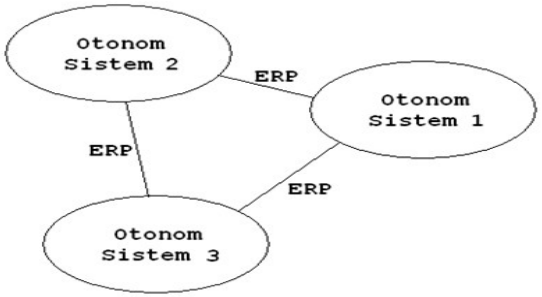
2- Statik yapılandırma : Hedef bilgisayar ağına bağlantı kurulabilmesi için tablo el ile doldurulur. Küçük ve yapısı değişmeyen ağlarda bu yöntem kullanılabilir.

- IP datagram yönlendirme bilgilerinin routerlar arasında değişiminin etkin bir şekilde gerçekleşmesi için yönlendirme protokolları tanımlanmıştır. Bu protokolların devamlılığını sürdürebilmesi için mesaj değişiminin sürekli olması gerekir.

DATAGRAM Yönlendirme protokolları

- Otonom sistemlerin kendi içindeki, temel yönlendirme değişim bilgisi için kullandıkları protokollara IGP(Interior Gateway Protokolu) denir.
- Otonom sistemler arasındaki haberleşme için kullanılan routerların temel yönlendirme değişim bilgisi için kullandıkları protokollara EGP(Exterior Gateway Protokolu) denir.





IGP Protokollarından en çok bilinenleri

-RIP (Routing İnformation Protocol - Yönlendirme Bilgi değişimi protokolu) : Tablolarını güncellemek için Uzaklık Vektör **(Distance Vector)** Algoritması kullanır.

-OSPF (Open Shortest Path First- İlk önce en kısa yolu seç): Tablolarını güncellemek için **Link State** algoritmasını kullanırlar.

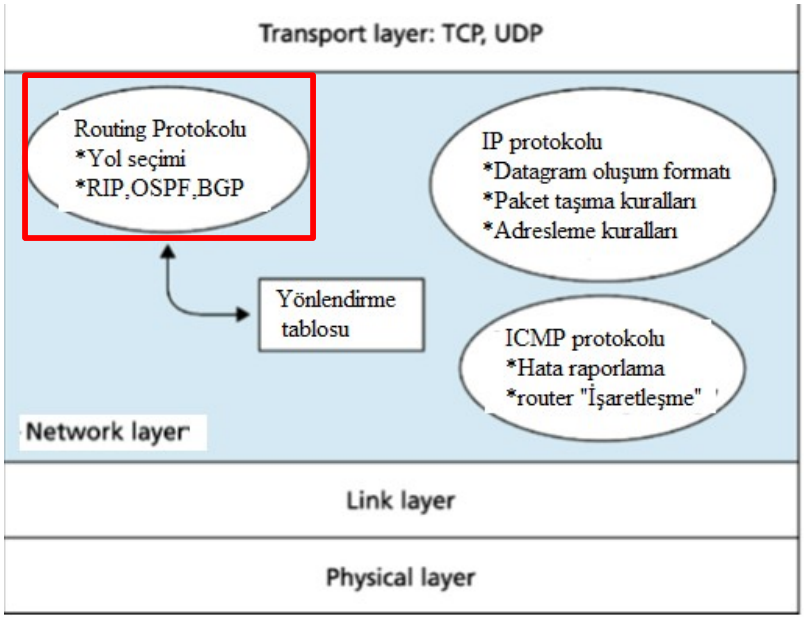
EGP Protokollarından en fazla bilineni;

-BGP (BGP(Border Gateway protocol – Sınır geçit protokolu)

- Yönlendiriciler arasında, yönlendirme bilgileri IP datagramlar aracılığı ile taşınır. Yönlendirme protokolları IP, TCP,UDP protokollarını kullanarak mesaj alış-verişini gerçekleştirir.

- ***OSPF Protokolu :*** IP datagramalarını kullanarak
- ***RIP Protokolu :*** UDP protokolunu kullanarak;
- ***BGP protokolu:*** TCP protokolunu kullanarak

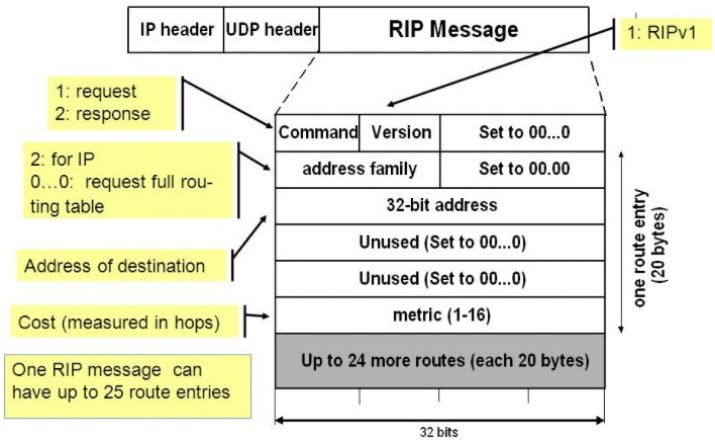
Yönlendirme bilgisi mesaj alış-verişini sağlarlar.



ROUTİNG Protokolu Saldırıları

* RIP spoofing ile roturdaki veya hosttaki rota tabloları değiştirilebilir. İstek mesajı ile rota tabloları kolaylıkla ele geçirilebilir.

RIP v.1 Paket Formatı



ROUTİNG Protokolu zayıflıkları

Routing protokolu seçenekleri RIP, IGRP, EIGRP, OSPF, BGP'dir. BGP, otonom ağlar içi ve ağlar arası iletişim için defacto yönlendirme standardıdır. RIP, IGP, OSPF, otonom ağlardaki iç yönlendirmede kullanılan protokollerdir.

* RIP Protokolu : UDP protokolunu kullanarak;
* BGP protokolu: TCP protokolunu kullanarak
* OSPF Protokolu: IP datagramlarını kullanarak yönlendirme bilgisi mesaj alış-verişini sağlarlar

* RIP datagramları dahili sıra nosu içermez ve kimlik doğrulaması (v.1) yoktur. Datagram gizliliği yoktur. UDP tabanlıdır (genellikle 520 portunu kullanır) ve durumsuzdur, yani, talep edilmemiş olsa da sahte cevap paketleri kabul edilir ve işlenir.
* IP sahtekarlığı saldırısını kullanan herhangi bir saldırgan, yetkili bir BGP istemcisi olarak maskelenen yarı çift yönlü bir BGP oturumu üretebilir.
* OSPF sadece kimlik doğrulama sağlar, gizlilik sağlamaz.

ICMP (İnternet Control Message protocol) Protokolu

IP protokolu bağlantısız bir protokol olduğundan, ağda seyahat eden datagramların iletim ve teslimat sürecinde meydana gelen beklenmedik hata, uyarı, kontrol bilgilerinin alışverişi için ICMP protokolu kullanılır. Daha çok routerlar tarafından kullanılır. ICMP protokolu ağ hakkında bilgi sahibi olmak için de kullanılır (istek/cevap). ICMP iletileri IP datagramları içerisinde kapsüllenerek seyahat eder. Yani ICMP, IP protokolunun dahili bir parçasıdır ve her IP modülünde mevcuttur.

• **ICMP mesajları iki ana kategoriye ayrılır.**

***Sorgu mesajları :** Bilgisayar veya ağ testleri için veya ağ özelliklerinden bilgi elde etmek için ICMP mesajları kullanılır (ping, traceroute komutları v.b).

- İstekler (Requests)

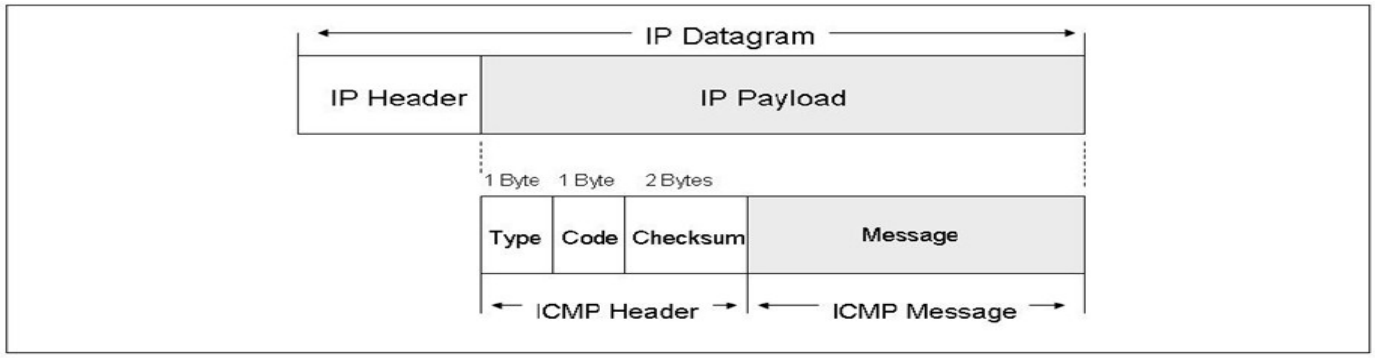
- Yanıtlar (Responses - reply)

*** Hata mesajları** : ICMP hata mesajını ağdaki tüm cihazlar, routerlarda dahil olmak üzere işleyebilir (Switchler işleyemez).

ICMP Hata mesajları aşağıdaki durumlarda üretilir.

- IP datagramların hedefe ulaşamaması durumunda
- Ağ geçitlerinin, datagramları hedefe yönlendiremeyecek kadar yoğun olmaları durumunda
- Datagramların hedeflerine gidebileceği daha uygun bir yol olması durumunda.
- Routerlar, datagramları yönlendirirken oluşabilecek problemleri bildirmek için
- Bilgisayarlar; protokol ve servis problemleri yaşadıkları zaman.
- **Sadece IP datagramlarla ilgili olaylarda ICMP mesajı üretilir.**
- Parçalanmış IP datagramlarda oluşacak hatalarda sadece ilki için ICMP mesajı iletilir.
- ICMP mesajlarının seyahat ile ilgili problemler için ICMP mesajı üretilmez.

ICMP Mesaj Formatı



ICMP header : **ICMP mesaj başlığı - 4 byte'tır.**

Type (Tür) : **ICMP mesajının türü - 1 byte,**

Code (Kod) : **ICMP mesajının alt türü, mesajı daha detaylı tanımlamak için -1 byte)**

Checksum : **ICMP mesajı için doğrulama, IP cehecsum'a benzer – 2 byte**

ICMP message : **Ek veri yoksa, 4 byte'lık 0 değeri olur.**

Her ICMP mesajı en az 8 bayttır.

Çok kullanılan ICMP Mesajları

Type

0 Echo Reply (Yankı): hedefin ulaşılabilir olduğu denetimi için.

3 Destination Unreachable: hedefin erişilemez olduğunu belirler

4 Source Quench: Rotadaki router'ın çok yoğun olduğunu belirtir.

5 Redirect: Routerlar rota belirlemek için kullanır.

8 Echo Request

11 Time Exceeded : Zaman aşımı- TTL'in 0'landığı bilgisi

12 Parameter Problem : IP datagramda oluşan problemleri bildirir.

13 Timestamp :Paketlerin iki nokta arasındaki gidiş geliş süreleri için.

14 Timestamp Reply:

15 Information Request

16 Information Reply

ICMP mesajlarını kullanan programlar

Ping ve *traceroute* uygulamaları ICMP protokolunu kullanır.

•***Ping:*** En çok kullanılan ağ analiz programlarından birisidir. Ping, hedef bilgisayara **"yankı istek (echo request) -** Type 8" mesajı gönderir. Eğer hedef bilgisayardan süresi içerisinde **"yankı cevap (echo reply)-** Type 0 **"** yanıtı gelirse, Ağ üzerinde erişilebilir olduğu anlaşılır.

•Ping her gönderdiği mesaj üzerine gönderilme zamanını ekler. Alınan yanıtı kullanarak (kaynak-hedef-kaynak dönüş süresi) paket iletimi için geçen zamanı bulabilir. Ping isteğine cevap için bir süre belirlenmiştir (time out- ping request time out -yaklaşık 2 sn).

* Hedef IP'ye Ping request'tan sonra time out kadar zaman içinde cevap (reply) gelmezse ping time-out hatası verir. Bu süreden sonra host dinlemeyi keser.

•Ping atılacak IP adresi için ARP tablosunda veya ARP sorgusunda IP-MAC eşleşmesi oluşturulamıyorsa ping request mesajı bile gönderilmez ve 'destination host unreachable – Hedef bilgisayar erişilemez ' hatası verir.

ping 192.15.36.44

Gidiş dönüş başarıyla tamamlanmadıysa, ping aracı çeşitli hata mesajları görüntüler. Ping mesajında alınan hata mesajları aşağıdaki bilgileri içerir:

•**Geçiş Süresinde TTL Süresi Doldu:** Bir IP paketi hedefine ulaşmamışsa, önce ağ üzerinde yaşayabileceği maksimum süreyi belirler. Bu hatayı gidermek için, ping -i anahtarını kullanarak TTL değerini artırılabilir.

•**Hedef Ana Bilgisayar Ulaşılamaz:** Hedef pasiftir veya ağda yoktur. Hedef ana bilgisayar için yerel veya uzak bir rota bulunmaması nedeniyle oluşabilir. Bu hatayı gidermek için yerel rota tablosunu değiştirilmesi veya düğümü aktif edilmesi.

•**İstek Zaman Aşımına Uğradı:** Ping komutunun zaman aşımına uğradığını gösterir. Ağ trafiği, Adres Çözümleme Protokolü (ARP) istek paketi filtreleme hatası veya yönlendirici hatası nedeniyle yankı mesajı alınmadığını gösterir. Ping-w seçeneğinden bekleme süresini artırmak, bu sorunu çözebilir.

•**Bilinmeyen Ana Bilgisayar:** IP adresinin veya ana bilgisayar adının ağda bulunmadığını veya hedef ana bilgisayar adının çözülemediğini belirtir. Bu sorunu gidermek için, etki alanı adı sistemi (DNS) sunucularının adını ve kullanılabilirliğini doğrulayın .

Başarılı ping

1	0.000000	Private_66:68:00	Broadcast	ARP	64 Who has 192.168.10.2? Tell 192.168.10.1
2	0.001007	Private_66:68:02	Private_66:68:00	ARP	64 192.168.10.2 is at 00:50:79:66:68:02
3	0.017249	192.168.10.1	192.168.10.2	ICMP	98 Echo (ping) request id=0x1c65, seq=1/256, ttl=64 (reply in 4)
4	0.017249	192.168.10.2	192.168.10.1	ICMP	98 Echo (ping) reply id=0x1c65, seq=1/256, ttl=64 (request in 3)
5	1.041118	192.168.10.1	192.168.10.2	ICMP	98 Echo (ping) request id=0x1d65, seq=2/512, ttl=64 (reply in 6)
6	1.041118	192.168.10.2	192.168.10.1	ICMP	98 Echo (ping) reply id=0x1d65, seq=2/512, ttl=64 (request in 5)
7	2.059236	192.168.10.1	192.168.10.2	ICMP	98 Echo (ping) request id=0x1e65, seq=3/768, ttl=64 (reply in 8)
8	2.059236	192.168.10.2	192.168.10.1	ICMP	98 Echo (ping) reply id=0x1e65, seq=3/768, ttl=64 (request in 7)
9	3.084413	192.168.10.1	192.168.10.2	ICMP	98 Echo (ping) request id=0x1f65, seq=4/1024, ttl=64 (reply in 10)
10	3.084413	192.168.10.2	192.168.10.1	ICMP	98 Echo (ping) reply id=0x1f65, seq=4/1024, ttl=64 (request in 9)
11	4.123826	192.168.10.1	192.168.10.2	ICMP	98 Echo (ping) request id=0x2065, seq=5/1280, ttl=64 (reply in 12)
12	4.123826	192.168.10.2	192.168.10.1	ICMP	98 Echo (ping) reply id=0x2065, seq=5/1280, ttl=64 (request in 11)

```
> Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:02 (00:50:79:66:68:02)
> Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x03a6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 7269 (0x1c65)
    Identifier (LE): 25884 (0x651c)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 4]
  > Data (56 bytes)
```

```
0000  00 50 79 66 68 02 00 50  79 66 68
0010  00 54 65 1c 00 00 40 01  80 39 c0
0020  0a 02 08 00 03 a6 1c 65  00 01 08
0030  0e 0f 10 11 12 13 14 15  16 17 18
0040  1e 1f 20 21 22 23 24 25  26 27 28
0050  2e 2f 30 31 32 33 34 35  36 37 38
0060  3e 3f
```

Wireshark · Packet 2 · -

```
> Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
> Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:00 (00:50:79:66:68:00)
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.1
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x43a4 [correct]
    [Checksum Status: Good]
    Identifier (BE): 58470 (0xe466)
    Identifier (LE): 26340 (0x66e4)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 1]
    [Response time: 0,000 ms]
  v Data (56 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f…
      [Length: 56]
```

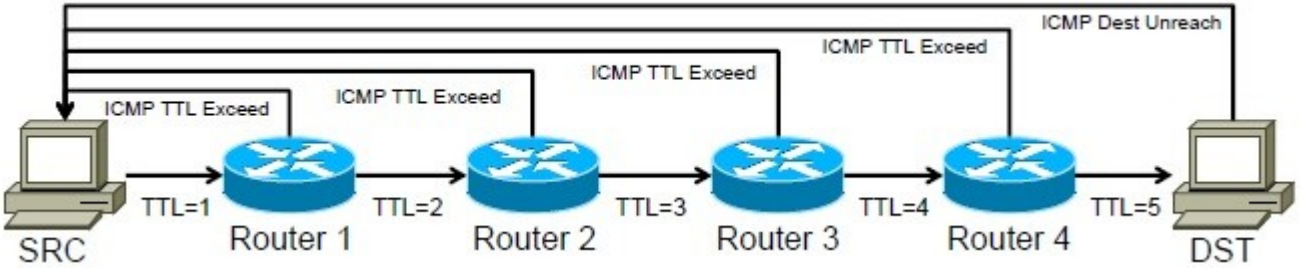
```
0000  00 50 79 66 68 00 00 50  79 66 68 02 08 00 45 00   ·Pyfh··P yfh···E·
0010  00 54 66 e4 00 00 40 01  7e 71 c0 a8 0a 02 c0 a8   ·Tf···@· ~q·····
```

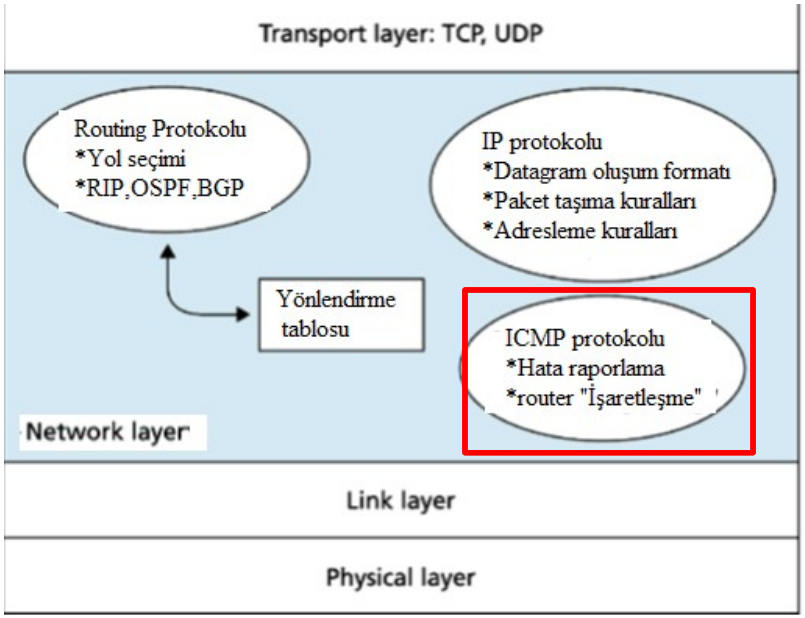
kali - PuTTY

```
kali> show ip

NAME          : kali[1]
IP/MASK       : 192.168.10.1/24
GATEWAY       : 255.255.255.0
DNS           :
MAC           : 00:50:79:66:68:00
LPORT         : 10014
RHOST:PORT    : 127.0.0.1:10015
MTU:          : 1500

kali> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=64 time=1.372 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=64 time=1.451 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=64 time=1.504 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=64 time=1.475 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=64 time=1.546 ms
```

Traceroute

- **<u>Traceroute:</u>** Datagramların hedeflerine ulaşıncaya kadar izledikleri rotanın belirlenmesi için kullanılan bir analiz programı (komutu)dır. Kaynak; paketin geçtiği yollarda karşılaştığı ağ elemanlarını öğrenmek için önce TTL değerini 1 yaptığı paketi gönderir. İlk ağ elemanı bu paketi alır almaz ICMP Type 11 (Time Exceeded) mesajını kaynağa gönderecektir. Traceroute bu mesajdan ilgili ağ elemanını tespit eder. Daha sonra TTL = 2 vererek paketi tekrar gönderir. Bu kez paket ilk elemanı aşarak ikinci elemandan ICMP Time Exceeded alır ve bunu da kaydeder. Bu şekilde hedef sunucuya kadar TTL değeri artırılarak bütün ağ elemanları tespit edilmiş olur.
- Time Exceeded mesajları da iç ağlar hakkında dış dünyaya bilgi vermemek üzere güvenlik gerekçesi ile devre dışı bırakılabilir.





ICMP Protokolu zayıflıkları

*ICMP kimlik doğrulaması sunmaz.
*IP protokolunun içerisindedir. IP'nin Kontrol ve hata mesaj protokoludur.

ICMP protokolu Saldırıları

* ICMP, ağdaki cihazları tarama ve istismar etmek için kullanılabilir.
*ICMP kullanımı ile, backdoor, port scan, redirect trafik, echo gibi DoS atakları düzenlenebilir

Genel ICMP Echo Atakları

- Ping (ICMP ile gerçekleşir) bombardımanı saldılarının amacı, büyük miktarda ICMP yankı istek paketlerini ağa yollayarak bant genişliğini kullanıp ağ kaynaklarını tüketmektir.

- Alınan her ICMP yankı istek (request) paketine karşılık, ICMP yankı cevap paketinin de yayınlandığına dikkat ediniz.

- Özellikle bant genişliği düşük olan ağlarda bu ataklar önemlidir.

Footprinting (Ping taraması)

- Hedef ağa saldırıdaki ilk adım, ağ hakkında bilgi toplamaktır. Buna 'ağın ayak izi‘ belirlemesi denir. ICMP bunun için uygundur. Bir ping taraması (sweep) ağa doğrudan bir saldırı değildir, ancak kesin bir tehditdir.
- Ping Taraması: Tanımlanmış bir IP aralığı için ağda hangi bilgisayarların canlı olduğunu bulmak için kullanılabilecek bir tekniktir. ICMP'ye izin veren ağ yöneticileri, ICMP tabanlı saldırılara karşı savunmasızdır.
- Birçok ağ yöneticisi, bu tür ayak izlerini önlemek için ICMP'yi tamamen engeller. Bu, sorun gidermeyi ve izlemeyi biraz zorlaştırdığından, bazı olumsuz yanları da vardır.
- Ping sweep için nmap, sing, ICMPscan v.b birçok araç mevcuttur. Bunlardan en çok kullanılanı nmap aracıdır. Windows tabanlı bir makinada;

```
$ nmap -sP -PI 192.168.0.0/24

Starting Nmap 4.10 ( http://www.insecure.org/nmap/ ) at 2007-04-01 20:
Host 192.168.0.0 seems to be a subnet broadcast address (2 extra pings
Host 192.168.0.1 appears to be up.
Host 192.168.0.25 appears to be up.
Host 192.168.0.32 appears to be up.
Host 192.168.0.50 appears to be up.
Host 192.168.0.65 appears to be up.
Host 192.168.0.102 appears to be up.
Host 192.168.0.110 appears to be up.
Host 192.168.0.155 appears to be up.
Host 192.168.0.255 seems to be a subnet broadcast address (2 extra pir
Nmap finished: 256 IP addresses (8 hosts up) scanned in 17.329 seconds
```

Port Scanning

- ICMP, “hangi portların açık olduğunu keşfetmek için”, saldırganlar tarafından büyük oranda kullanılır. Çünkü TCP protokolu gibi bağlantılı bir protokol olmadığından saldırganlar için paha biçilmez bir araçtır.
- İlgili bilgisayardaki bir port’a bir UDP paket gönderilmesi ile portun açık olup olmadığını bildiren bir ICMP yanıtı alırsınız.
  - Eğer port açık ise; bir cevap gelmeyecektir.
  - Eğer port kapalı ise; **ICMP *tip3* *code3* olan bir ICMP reply mesajı alınacaktır. (Hedef ulaşılamaz, Port ulaşılamaz)**.

Hping2 tool’unu kullanarak 192.168.5.5 IP’sinin 50.portuna bir UDP paketi gönderilsin;

```
[root@stan /root]# hping2 -2 192.168.5.5 -p 50 -c 1
default routing not present
HPING 192.168.5.5 (eth0 192.168.5.5): udp mode set, 28 headers + 0 data
bytes
ICMP Port Unreachable from 192.168.5.5  (kenny.sys-security.com)

--- 192.168.5.5 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

ICMP Nuke Atakları

- Bilgisayarlar çoğu zaman aralarındaki bağlantının sağlamlığını birbirlerine ICMP paketleri göndererek anlarlar.
- **ICMP Nuke Atağı;** Sahte adresler (spoof edilmiş) kullanarak, bir saldırgan; iki host arasındaki düzgün iletişimi "**Time Exceeded**" (Type 11) veya "**Destination Unreachable**" (ICMP Type 3) mesajlarını her iki hosta'da göndererek, sanki hata varmış gibi gösterebilir, bozabilir.
- Bu bir DOS atağıdır. Eski bir atak türüdür.
- ICMP Types and Codes 'lar konusuna bir gözat.

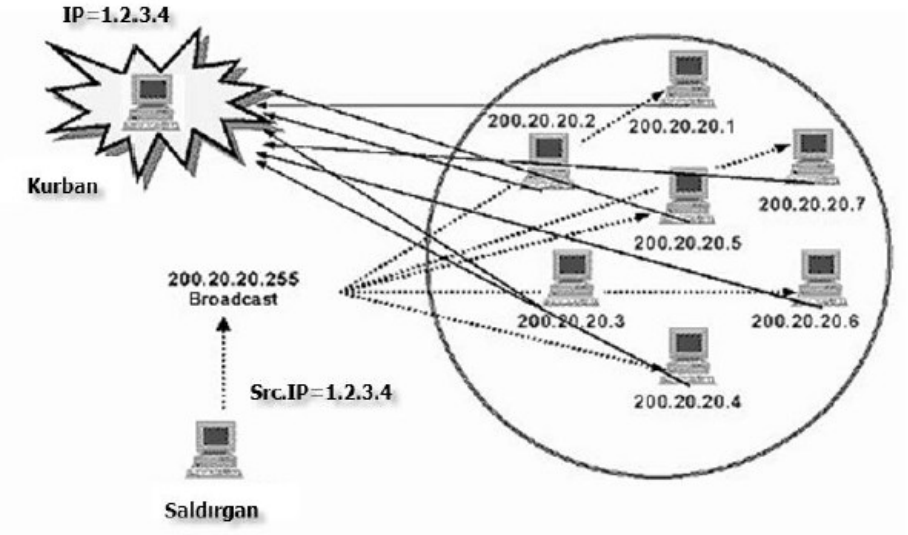
ICMP Flood (ICMP Taşkını-Sel basması Bombardımanı)

- Ping Flood, bir ping (ICMP üzerinden yapılır) broadcast fırtınası yaratarak hedef sistemi bunaltabilir. Bu bir DoS saldırısıdır.
- Linux'ta, ping –f kullanılarak herhangibir host'a bir taşkın oluşturulabilir.

```
root@router# ping -f 10.10.10.12 -c 1000
```

ile 10.10.10.12 IP'li host'a 1,000 paket gönderilir.

IP ping paketinin işleyişinden yararlanan "***Smurf saldırıları***" da ICMP FLOOD'un özel bir halidir. Çok sayıda reply paketi ile hedefin gerçek trafiği alması engellenir. Smurf ataklarında; kurban bilgisayarın IP adresinden network'ün broadcast adresine Internet (ICMP) isteği (ping) gönderilir ve network üzerindeki bütün bilgisayarlardan kurban bilgisayara yanıt göndermesi sağlanır.



Ping Flood'dan korunma

- Ping flood, IPTable 'ın konfigirasyonu ile "ICMP echo-request messages" larının sayısını sınırlayarak durudurulabilir.

```
root@router# iptables –A FORWARD –p icmp –icmp-
  type echo-request -m limit –limit 10/s –j
  ACCEPT
(saniyede 10 tane  gelen icmp echo request paketlerini kabul et)

root@router# iptables –A FORWARD –p icmp –icmp-
  type echo-request –j DROP
(Icmp echo-request paketlerini düşür)
```

Not:iptables, Linux veya Unıx'te NAT'lama veya paket filtreleme için bir araçtır.

Ping of Death

- Ping of Death, IP paketlerine gömülü olarak ICMP ile gönderilen “echo request” mesajları ile yapılır. Bu mesajlar 65.535 bayt’tan daha büyük mesajlar halinde sürekli olarak gönerilirse Buffer kapasitesi küçük olan makinalarda buffer taşmasına sebep olarak makinanın çökmesine sebep olur. Ping of death bir DoS atağı çeşididir.

Windows komut satırından:

ping -1 65550 192.168.1.X

Linux komut satırından:

ping -s 65550 192.168.1.X

SMURF Atağı

Daha önce tartıştığımız gibi, ne zaman bir tip 8 gönderilirse, bir tip 0 geri gönderilir veya bir yankı isteği gönderildiğinde bir ICMP yankı yanıtı gönderilir. Bir smurf saldırısında, saldırgan ICMP paketinin kaynak adresini bozar ve bu ağdaki tüm bilgisayarlara bir yayın gönderir. Ağ aygıtları bu trafiği filtrelemezse, ağdaki tüm bilgisayarlara yayınlanır. Mağdurun ağı, bu kadar fazla trafikten etkilenir ve bu da tüm ağın verimliliğini düşürür.

Adres sahtekarlığını önlemek için yönlendiricilere ve güvenlik duvarına filtreler yerleştirin. Bir LAN segmentine bir IP adresi atanmalı ve kaynak makinenin IP adresi segmente atanmış IP adresi aralığında değilse, trafik kesilmelidir.

ICMP Router keşfi

ICMP router bulma protokolü, komşu yönlendiricilerin IP adresini bulur. Yönlendirici bulma mesajı, Ana bilgisayarların komşu bir yönlendiricinin varlığını keşfetmesine olanak tanır, ancak hangi yönlendiricinin belirli bir hedefe ulaşmak için en iyisi değildir. Yönlendirici reklam mesajı (hello mesaji v.b) bir ICMP mesajıdır (tip 9, kod 0). ICMP yönlendirici bulma protokolü için temel zorluk, herhangi bir kimlik doğrulama biçiminin bulunmamasıdır, bu nedenle son ana makinelerin aldıkları bilgilerin geçerli olup olmadığını söylemeleri imkansızdır.

Yukarıdaki sorun nedeniyle, saldırgan, saldırganın kaynağından uç noktaya kadar olan tüm iletişim için orta saldırgan olarak hareket edeceği man in the middle gerçekleştirebilir. Saldırganlar ayrıca ICMP yönlendirici bulma mesajlarını taklit edebilir ve kurbanın yönlendirme tablosuna uzaktan kötü rota girişleri ekleyebilir. Bu tür saldırılar DOS saldırısına yol açabilir ve oldukça şiddetli olabilir.

ICMP rota keşiflerini önlemek için kullanılan bir önlem, dijital imzaları kullanmak ve tüm tip 9 ve 10 ICMP paketlerini engellemektir

Genel bakış

- IP, ICMP, and Routing protokolları önemlidir.
- IP bağlantısız bir protokol olduğu için DOS saldırılarına açıktır.
- Saldırganlar tarafından IP protokoluna saldırılar için ICMP kullanılabilir.
- Routing protokolları data yığınlarına maruz kalırlar.

BMÜ-457 Ağ Güvenliği

8.Hafta

OSI 4.katman (Transport - İletim layer) Güvenliği

TCP Protokolu

- TCP protokolu; bilgisayarlarda çalışan uygulamalar arasında;

  <İstemci IP adresi, Port No>, <Sunucu IP adresi, Port no> ikililerini temel alan bağlantı kurar. Her TCP bağlantısı bu ikililerle ifade edilir.
- IP protokolu bağlantısızdır. Dolayısıyla gönderilen paketlerin yerlerine ulaştığını garanti etmez. Bu açığı kapatmak için, bağlantılı ve güvenli veri akışını sağlayan TCP protokoluna ihtiyaç duyulur.
- TCP protokolunu kullanan uygulamalar veri göndermeden önce bağlantı kurmak zorundadaırlar.
- TCP , bağlantıda olan bilgisayarlar arasındaki güvenli veri iletişimini sağlayan, sanal devre mantığıyla çalışan bir protokoldur.
- **Hata denetimi yapar**
- **Güvenli veri iletimi sağlar.**
- **Bağlantıda olan bilgisayarlar arasında akış, tıkanıklık kontrolu sağlar.**
- **Çoklama (Multiplexing) yöntemiyle birden fazla bağlantıya izin verir.**
- **Sadece bağlantı kurulduktan sonra veri iletimi sağlar.**
- **Gönderilen mesajlar için, öncelik, güvenlik tanımlamaları yapılabilir.**

PORT KAVRAMI

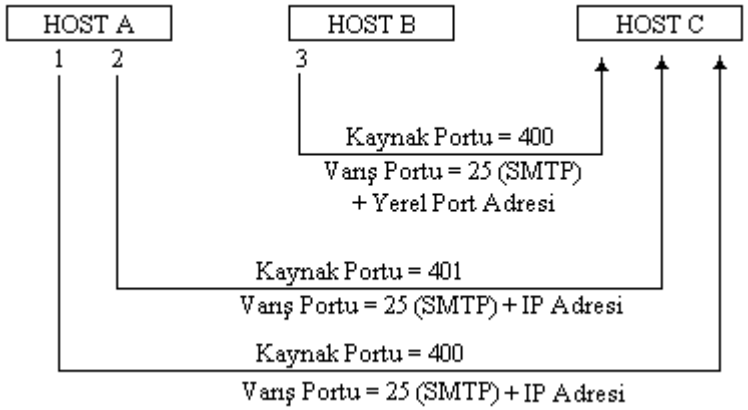
- Bir Hos'tun diğer host üzerindeki değişik servisleri (hizmetleri) kullanabilmesi için veya değişik bilgisayarların aynı bilgisayardaki bir servisi kullanabilmesi için bu servisi tanımlayan adreslemeler vardır.

- TCP protokolunda her uçta 2^{16} tane farklı TSAP adresi tanımlıdır. Bu adreslere PORT denir.

- Uç düğümün 32 bitlik IP adresi ve 16 bitlik port adresinin beraber kullanılmasına soket no denir. Bir soketin blok şeması aşağıda verilmektedir.

Port atama -3

- Başka bir host`un C host`una aynı kaynak ve varış port değerleri ile bir bağlantı isteği göndermesi olasıdır. Varış port değerlerinin aynı olması olağandışı değildir. çünkü iyi-bilinen portlara sıklıkla ulaşım isteği vardır. Bu durumda, varış portu 25 SMTP`yi tanımlayacaktır. Kaynak port tanımlayıcıları bölgesel bir olay olduğundan Şekil'de gördüğümüz gibi B host`uda kaynak portunu 400 olarak seçmiştir.
- Ek bir tanımlayıcı olmaksızın, A ve C host`ları arasındaki ve B ve C host`ları arasındaki bağlantılarda çakışma olacaktır çünkü her iki bağlantı da aynı varış ve kaynak port numaralarını kullanmaktadır. Bu gibi durumlarda, C host`u datagramların IP başlıklarındaki IP adreslerini kullanarak ayrımı kolayca başarır. Bu durumda kaynak portları ikilenir ancak internet adresleri oturumları farklılaştırır.



TCP Protokolu Mesaj Yapısı

Kaynak ve hedef portlar, servis noktalarının sağlanması içindir. İlk 1023 port no'su IANA tarafında kullanılan standart port nolarıdır.Uygulamalar diğer port nolarını diledikleri gibi seçerler.

Sıra (dizi) no ve onay (Ack-Bilgi) no kısımları bağlantı güvenliği için kullanılan parça sıra no ve alıcı tarafından beklendiği bildirilen (alıcı tarafında) parça no kısımlarıdır.

Bayrak alanı

ACK =1 bilgi numarasının geçerli olduğunu belirtir.

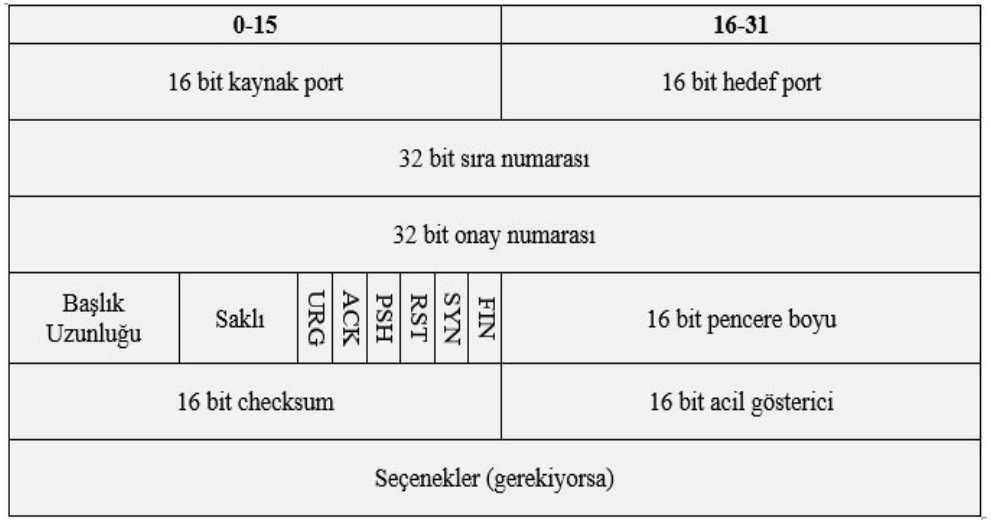
SYN =1 Bu durum TCP bağlantısının kurulacağını belirtir.

FIN =1 Bağlantının sonlanacağını bildirir.

RST = 1 bağlantının fazla hatalı olduğu, sonlandırılacağı anlamındadır.

PSH =1 TCP modülü aldığı veriyi acilen üst katmana gönderir.

URG =1 alıcıya, aldığı dataları işlemeden band dışı veri gönderilmesine izin verir.

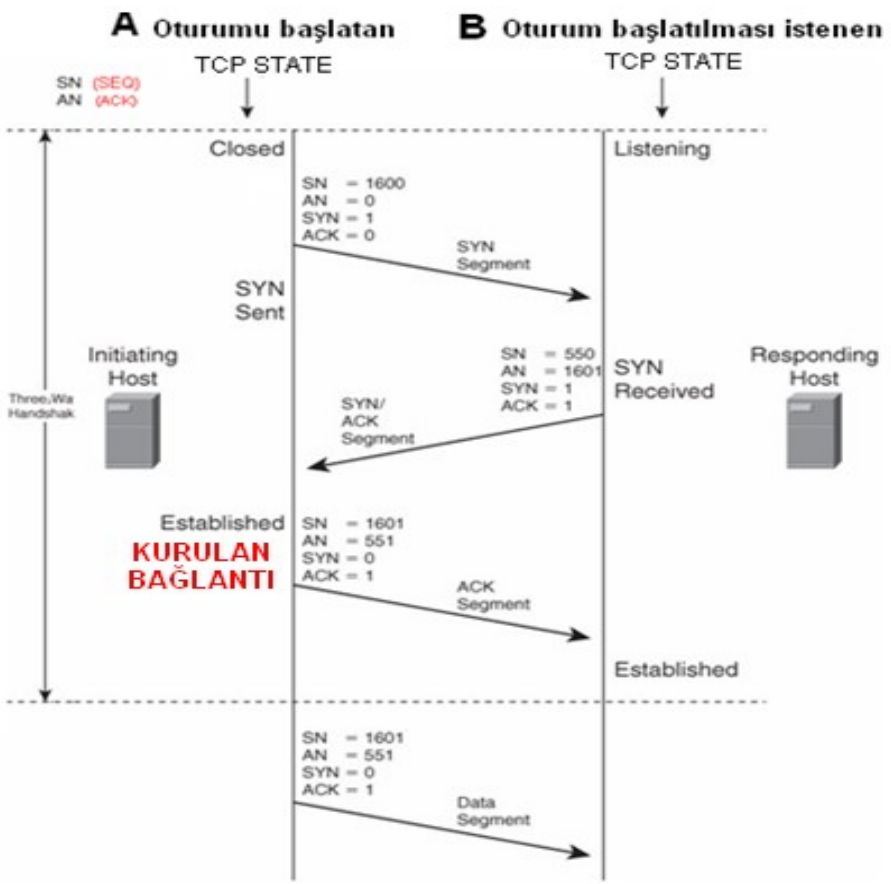


TCP bağlantıları,"üç adımda uzlaşma" **Three Way handshaking** yöntemiyle kurulur.

SYN=1 ve ACK=0 bağlantı açma isteği
SYN=1 ve SYN=1 bağlantı açma onayı
SYN=0 ve ACK=1 Veri Paketi veya ACK paketi

TCP protokolunda bağlantı açma (Three way handshake)

TCP bağlantı başlatma yordamı iletişim noktaları arasında üç paket iletim gerektirdiğinden genellikle üç-yollu el sıkışma denir. Başlatan bilgisayar **(A)**, yeni bağlantı için bir rastgele başlangıç sıra numarası (ISN –İnital service-sıra no) seçer ve daha sonra SYN biti=1 ve ACK biti =0 olarak ayarlanmış ilk paket gönderir. Bu pakete SYN denir



SYN alan **B** (yanıt veren), yeni bir bağlantı için bir ISN (Başlangıç dizi no- örn.550) seçer ve sonra **SYN biti=1 ve ACK biti =1** olacak şekilde cevap gönderir. Bu paket SYN / ACK Onay paketidir. ACK no alanına ise A (oturumu başlatan)'ın SYN paketindeki SEQ' no +1 yapar.

A bu SYN / ACK onay paketini aldıktan sonra; oturumun kabul edildiğini anlar. SYN bit=0 ve ACK biti= 1 yaparak, yeni segmenti B'ye gönderir. AN no'sunu 1 arttırır (551- Alıcının gönderdiği paketteki ISN No'sunu). Sıra Numarası (SN) alanına veri olmamasına rağmen, A'nın paketindeki ISN'yi bir arttırır. Bu ACK segmentinin tek amacı A ve B 'nin bu işle ilgili sayaçlarının senkronizasyonudur. Daha sonraki paketler veri taşır.

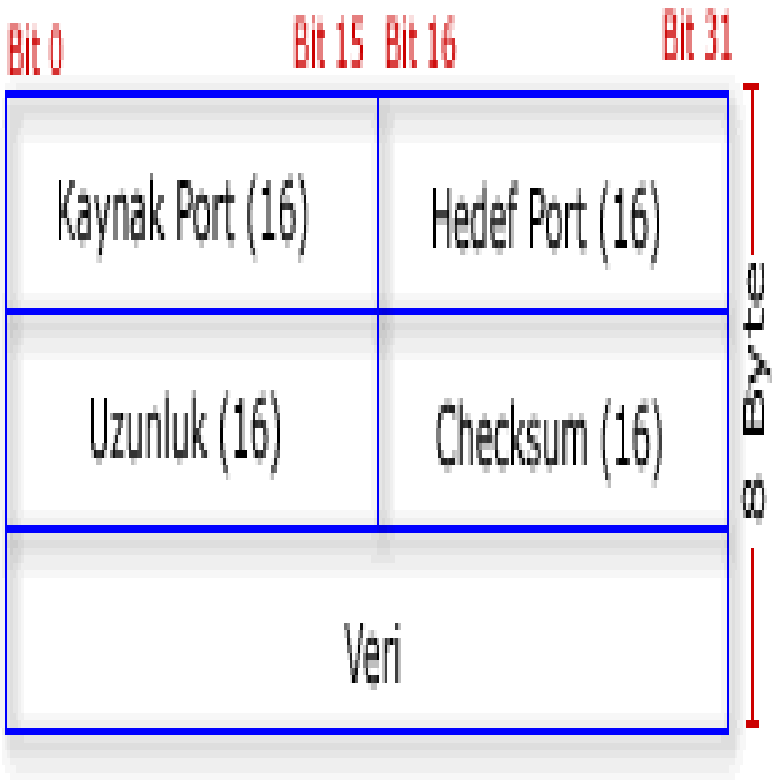
Kısa özet

Hizmet veren bir TCP portu açıksa kendisine gelen SYN paketine karşılık olarak ACK+SYN paketi döner. Dönen paketlerden ACK (onay paketi), SYN ise hizmet veren tarafın istek başlatma paketidir.

Port kapalıysa RST döner, SYNflood saldırısının başarılı olabilmesi için portun açık ve dinlemede (LISTEN mod) olması gerekir.

UDP paket formatı

- **kaynak port**: Opsiyonel bir alandır. Gönderilen işlemin portunu gösterir. Eğer gönderen host bir kaynak numarasına sahip değilse bu alan “0” ile doludur
- **hedef port:** Hedef host içerisinde, işlemlere uygun ayrımları yapmak için kullanılır. Hedef port internet adresleri parçalarının genel durumunu içerir.
- **Uzunluk:** UDP veri ve UDP başlığının bayt cinsinden toplam uzunluğudur.minimum 8 bayttır
- **Checksum:** IP ve UDP başlığı ve verinin bilgisini içeren yalancı başlığın toplamı olan birbirinin tamamlayıcısı 16 bitten oluşur. Opsiyonel bir alandır. Hata kontrol mekanizması sağlar. Eğer hata kontrolü yapılmayacaksa bu alan “0” ile doludur.
- **Veri:**Opsiyonel



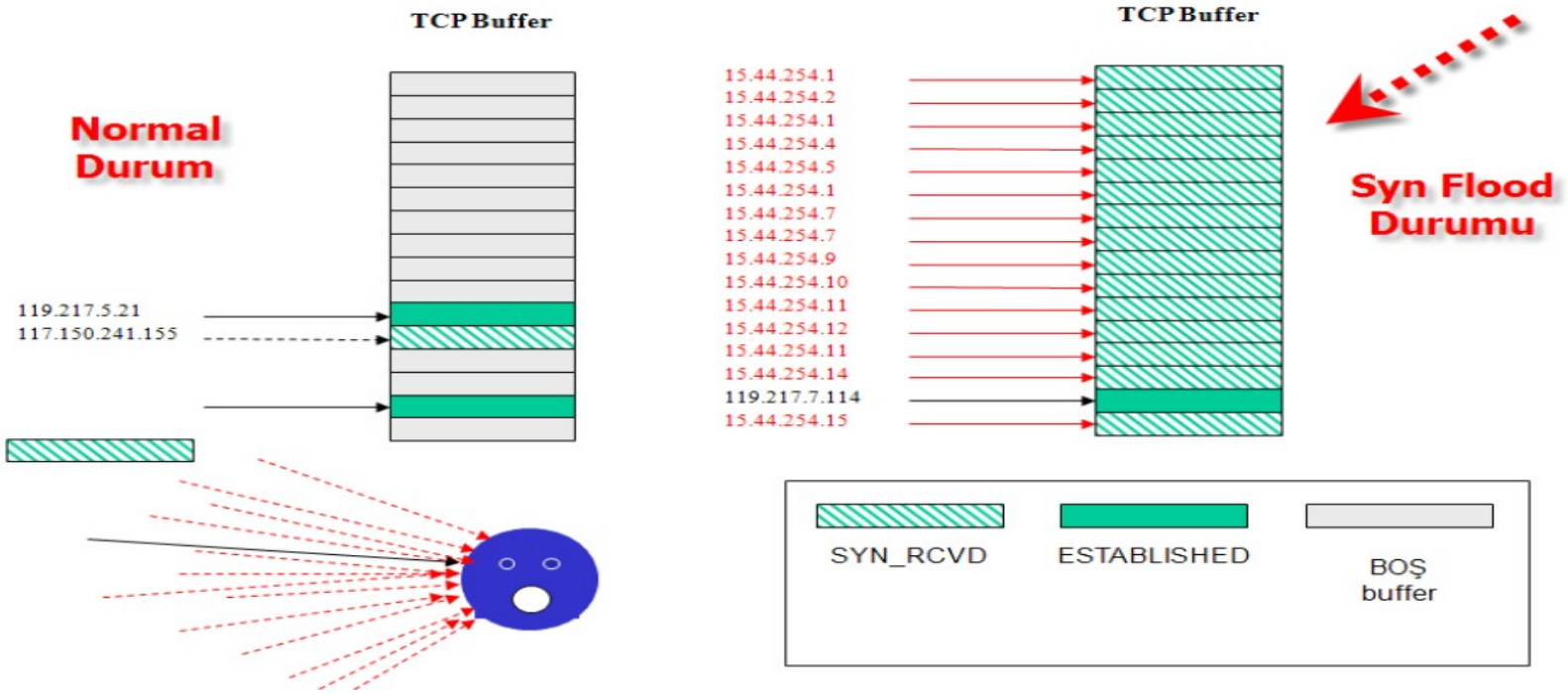
TCP protokoluna yönelik saldırılar

- TCP protokolunun tasarım özelliklerinden dolayı iki önemli zayıf noktası vardır.

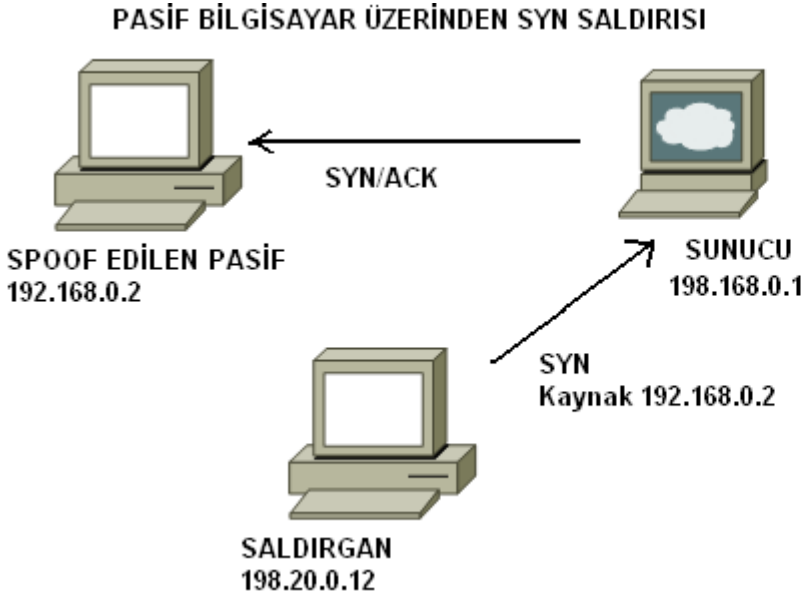
  - Protokol, TCP bağlantısı kurma isteği **"SYN Bombardımanı- SYN Flooding"** karşısında zayıf kalır : SYN flooding genellikle serverlara yapılan bir saldırı türüdür. Amacı çok sayıda "Bağlantı istek Paketi" hazırlayıp sunucuya göndererek hizmetleri aksatmaktır .

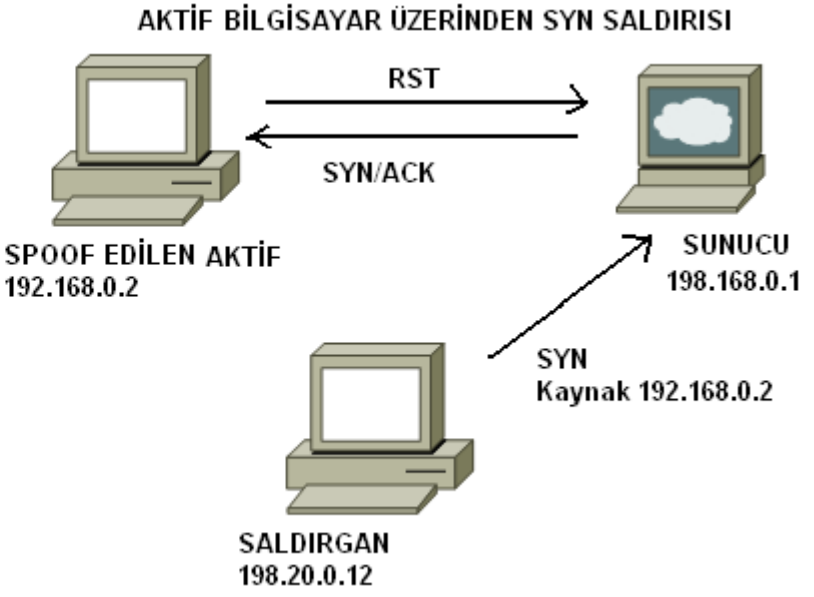
  - Protokol **"TCP oturumu ele geçirme "** saldırıları karşısında zayıf kalır. "TCP oturumunu ele geçirme"; iki bilgisayar arasında üç adımda sağlanan TCP bağlantısının birtakım yöntemlerle ele geçirilmesi veya veri akışına ; bağlantı içerisinde yer almaması gereken verileri eklemektir.

Syn Flood saldırısı, açık bir porta (dinlemede olan port), sistemin kapasitesinden fazla gönderilecek SYN paketleriyle gerçekleştirilir. Bu kapasiteye ***Backlog Queue*** denilmektedir. İşletim sistemleri aldığı her SYN paketine karşılık üçlü el sıkışmanın tamamlanacağı ana kadar bellekten bir alan kullanırlar, bu alan **TCB (Transmission Control Block)** olarak adlandırılır . Bu alanların toplamı **Backlog queue (Birikim kuyruğu)** olarak adlandırılır. Başka bir ifadeyle işletim sisteminin half-open olarak ne kadar bağlantı tutabileceğini «backlog queue» veriyapısı belirler. Bu değer her işletim sisteminde vardır ve ön tanımlı olarak düşük bir değerdir(256 gibi).
Synflood saldırılarında tüm mesele backlog queue'nin dolması ve yeni gelen bağlantıların reddedilmesidir. Backlog queue değerinin büyük olması demek daha fazla half-open(SYN paketi) bağlantı kabul edebilmek demektir. SYNFlood saldırılarında backlog değeri arttırılarak saldırıya karşı ek önlem alınabilir
Backlog queue dolmasıyla birlikte işletim sistemi yeni bağlantı kabul edemez ve bu esnada sunucuya bağlanmaya çalışanlar bağlanamazlar ki bu da SYN Flood saldırısına denk gelir.



- SYN flood saldırısı için spoof edilmiş (taklit edilmiş) IP datagramlar kullanılır. Yani bağlantı kurma istek segmentini taşıyan paketlerin gönderici IP'sine spoof edilmiş veya yapay olarak yaratılmış adresler atanır.
- Taklit edilmiş paketler ile pasif bigisayar saldırısı için, seçilen IP adresine, IP datagramların yönlendirilebilir olması fakat , bilgisayarın erişilebilir olmaması gerekir (Sunucu onay segmentini gönderip oturumun senkronizasyonunu sağlayan üçüncü paketi bekleyecektir.)
- Taklit edilmiş paketler için aktif bigisayar saldırılarında; Sunucunun gönderdiği SYN/ACK paketlerine, aktif bigisayar, RST =1 olan datagramlar gönderir. Bu paketi alan sunucu bağlantı isteğini sonlandırır. Hafızadaki yerini temizler.





Synflood Önleme Yöntem ve Çeşitleri

SynFlood saldırılarına karşı çeşitli önlemler geliştirilmiştir. Bunlar arasında önemlileri;

- Syncookie
- Syncache(FreeBSD default)
- SynProxy
- TCP Authentication

SynCookie

Normal TCP bağlantılarında gelen SYN bayraklı pakete karşılık ACK=1 ve SYN=1 paketi gönderilir. Gönderilen ikinci (sunucunun gönderdiği) SYN paketinde ISN (Sıra no) değeri random olarak atanır ve son gelecek ACK paketindeki sıra numarasının bizim gönderdiğimizden bir fazla olması beklenir, son paket gelene kadar da sistemden bu bağlantı için bir kaynak ayrılır (backlog queue).Eğer bizim gönderdiğimiz SYN paketine dönen ACK cevabı bizim ISN+1değilse paket kabul edilmez.

Syncookie aktif edilmiş bir sistemde gelen SYN paketi için sistemden bir kaynak ayrılmaz, bunun aksine SYN paketine dönecek cevaptaki ISN numarası özel olarak hesaplanır (kaynak.ip + kaynak.port + hedef.ip + hedef.port + x değeri) ve hedefe gönderilir, hedef son paket olan ACK'i gönderdiğinde ISN hesaplama işlemi tekrarlanır ve eğer ISN numarası uygunsa bağlantı kurulur, değilse bağlantı kurulmaz. Böylece spoof edilmiş binlerce ip adresinden gelen SYN paketleri için sistemde bellek tüketilmemiş olacaktır ki bu da sistemin SYNflood saldırıları esnasında daha dayanıklı olmasını sağlar.

Syncookie mekanizması backlog queue kullanmadığı için sistem kaynaklarını daha az tüketir. Syncookie aktif iken hazırlanan özel ISN numarası cookie olarak adlandırılır.

İstemci tarafı syncookie özelliği İnverse syn cookie (Scanrand aracı) araçları kullanılarak syncookie engellemesi aşılabilir. Bu durumda da bir ip adresinden gelecek max bağlantı sayısı limitlenerek saldırı engellenmiş olur.

Syncookie'de özel hazırlanacak ISN'ler için üretilen random değerler sistemde matematiksel işlem gücü gerektirdiği için CPU harcar ve eğer saldırının boyutu yüksekse CPU performans problemlerinden dolayı sistem yine darboğaz yaşar. DDOS Engelleme ürünleri(bazı IPS'ler de) bu darboğazı aşmak için sistemde Syncookie özelliğini farklı özel bir CPU'ya devredeler.

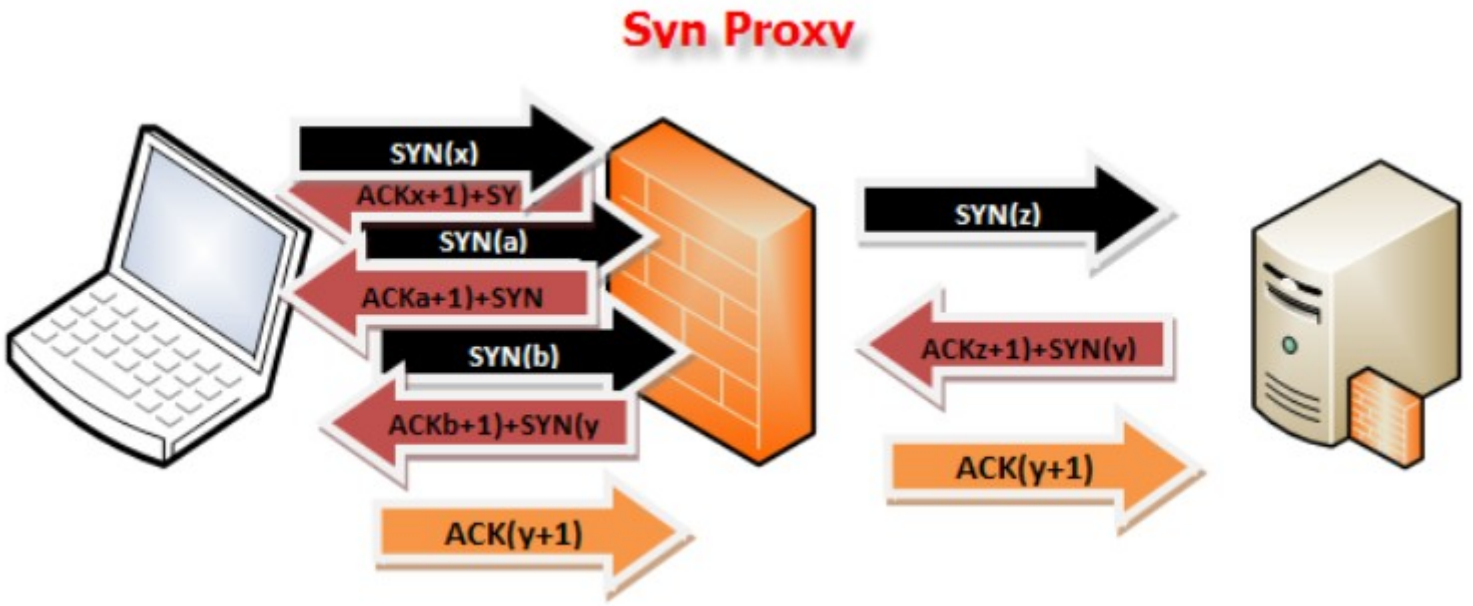
SynCache nasıl çalışır?

LISTEN modundanki bir portun gelen SYN paketlerinde bellekten bir alan ayırdığını ve bu alanın belirli boyutlarda olduğundan bahsetmiştik. SynCache özelliği , gelen SYN paketleri için TCB değerinden daha az yer kaplayan başka bir veri yapısı kullanmayı önerir. Böylece sisteme gelen SYN paketlerinde daha az bellek alanı harcanır(Normalde 700 Byte civarı, 160 Byte Syncache kullanıldığında).

Fakat yoğun bir saldırı da bu özellik kısa sürede işe yaramaz hale gelecektir. Bu sebepledir ki Syncache tek başına synflood saldırılarına karşı efektif bir koruma sağlamaz. Syncookie'i tetikleyici olarak kullanılır. Yani sistemde öntanımlı olarak syncookie aktif edilmez, syncache aktif edilir. Syncache belli bir değerin üzerinde SYN paketi almaya başladığında SYNCookie'ei tetikler vesistem koruma moduna geçer.

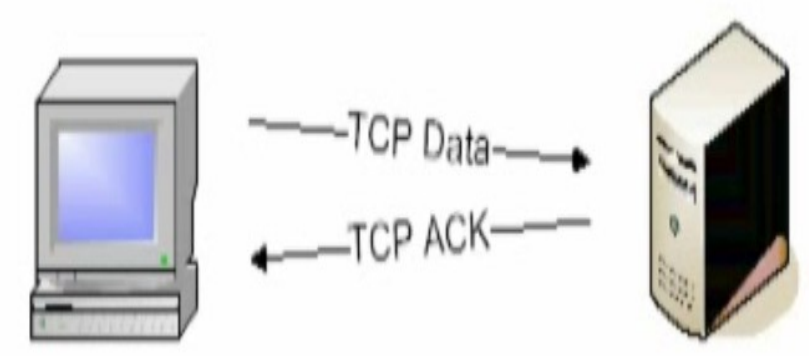
SynProxy

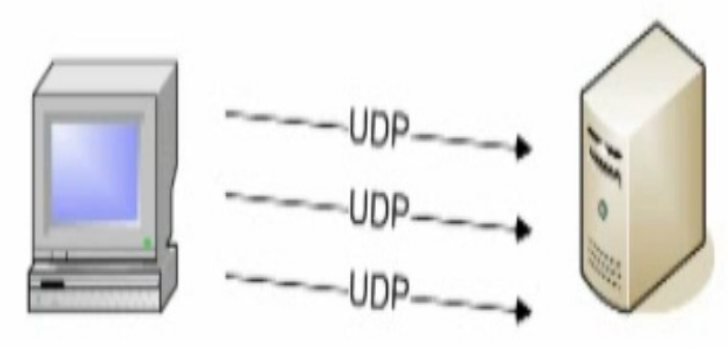
SynProxy, SYN paketlerine karşı proxylik yapmaya yarayan bir özelliktir. Güvenlik duvarlarında ve Syncookie'nin kullanımının sıkıntılı olduğu durumlarda rahatlıkla kullanılabilir. Syncookie gibi arkasında korumaya aldığı sistemlere gelecek tüm SYN paketlerini karşılar ve üçlü el sıkışma tamamlandıktan sonra paketleri koruduğu sistemlere yönlendirir



UDP Portlarından Saldırılar

- UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir, gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.





UDP Portlarından Saldırılar

- Bir bilgisayar üzerinde veya birkaç bilgisayar arasında,UDP portlarına yöneltilecek yoğun paket akışıyla gerçekleştirilen bu saldırılar, tek bir bilgisayar üzerinde gerçekleştiriliyorken bu bilgisayarın performansının düşmesine, birden fazla bilgisayar arasında gerçekleştiriliyorken ise, ağ performansının düşmesine sebep olacaktır.

- Birbiriyle haberleşmekte olan iki UDP servisinden birisi veya her ikisi üreteceği yoğun paket akışıyla, karşısındaki bilgisayarın servisini kilitlemeyi, bilgisayarın performansını kötüleştirmeyi başarabilir.

UDP Portlarından Saldırılar

- Örneğin 7 numaralı portu kullanan UDP **echo servisi**, karşısındaki bilgisayardan (istemci) aldığı bilgileri olduğu gibi geri gönderir.
- 19 numaralı port üzerinden servis veren UDP **chargen servisi** ise, istemci bilgisayardan her paket alışında, rastgele sayıdaki verilerden oluşan paketi geri gönderir.
- Bu iki servise ilişkin UDP portlarının aynı bilgisayar üzerinde veya değişik bilgisayarlar arasında birbirine bağlanması, sonsuz bir trafiğin oluşmasına sebep olacaktır.
- Bu hem servisi veren bilgisayarı hem de trafiğin aktığı ağı etkileyecektir.

UDP Portlarından Saldırılar

- Böyle bir saldırı sonucunda doğabilecek sonuçlar şunlardır:
  - Saldırının yöneltildiği servisler kilitlenebilir.
  - Bu servisleri veren bilgisayarların performansı düşebilir
  - Servisleri veren bilgisayarların bulunduğu ağın trafiğini arttırır.
- Bu saldırı tipinden korunmak için alınabilecek önlemlerin başında saldırıda kullanılan servisleri bilgisayarın üzerinden kaldırmak gelir.

UDP Portlarından Saldırılar

- Bu yaklaşımı kullanırken iptal edilecek servislerin ne kadar gerekli olduğu da önemlidir.

- Bu saldırılarda en çok kullanılan UDP servisleri **chargen** ve **echo** servisleridir. Bu servisler neredeyse hiç kullanılmazlar. Dolayısıyla bu servislerin iptal edilmesi ya da güvenlik duvarı üzerinden filtrelenmesi, normal çalışmayı etkilemeyecektir.

- Saldırıların daha çok hangi servislere yapıldığının tespiti için ağa saldırıları kontrol edip raporlayan programların kurulması faydalı olacaktır.

UDP Flood Saldırısı

- UDP Flood saldırısı host tabanlı servis dışı bırakma saldırılarından biridir.
- UDP Flood atağı saldırganın hedef sistemin rastgele bir portuna UDP paket göndermesiyle yapılır.
- Saldırgan, saldırının etkisini arttırmak için zombi bilgisayar denilen, saldırganın önceden üzerine casus yazılım yükleyerek ele geçirdiği sistemleri kullanır.
- Böylece hem kendi IP adresini saklamış olup yakalanma riskini azaltır hem de binlerce zombi bilgisayarı kullanarak atağın kuvvetini arttırır.

UDP Flood Saldırısı

- Hedef sistem bir UDP paket aldığında hedef portta hangi uygulamanın beklediği hesaplanır.
- Portta bekleyen uygulama olmadığı anlaşılınca erişilemeyen sahte IP adreslerine bir ICMP paketi üretilir ve her paket için 60 sn beklenir. Bu saldırı ağda tıkanıklık ya da kaynak doluluğuna sebep olur.
- UDP trafiğinin TCP trafiğine önceliği vardır. TCP protokolünün uzun sürede gelen paket onayları karşısında tıkanıklığı kontrol eden bir mekanizması vardır: bu mekanizma gönderme aralığını düzenleyerek tıkanıklık oranını azaltır.
- UDP protokolü bu mekanizmaya sahip değildir. Bir süre sonra tüm bant genişliğini kullanarak TCP trafiğine çok az yer bırakır.
- Eğer yeterli UDP paket hedef sistemdeki porta gönderilirse sistem çöker ve servis dışı bırakılır.

BMÜ-457 Ağ Güvenliği

9.Hafta

(TCP/IP v.4 7.katman)
Uygulama katmanı ve Açıkları
(Uygulama+Sunum+Oturum)

Bazı İnternet Uygulamaları

- E-posta
- Web
- Instant messaging
- Remote login
- P2P dosya paylaşımı
- Çok kullanıcılı ağ oyunları
- Streaming
- Internet telefon
- Real-time video konferans
- Paralel işlem

Ağ Uygulaması oluşturma

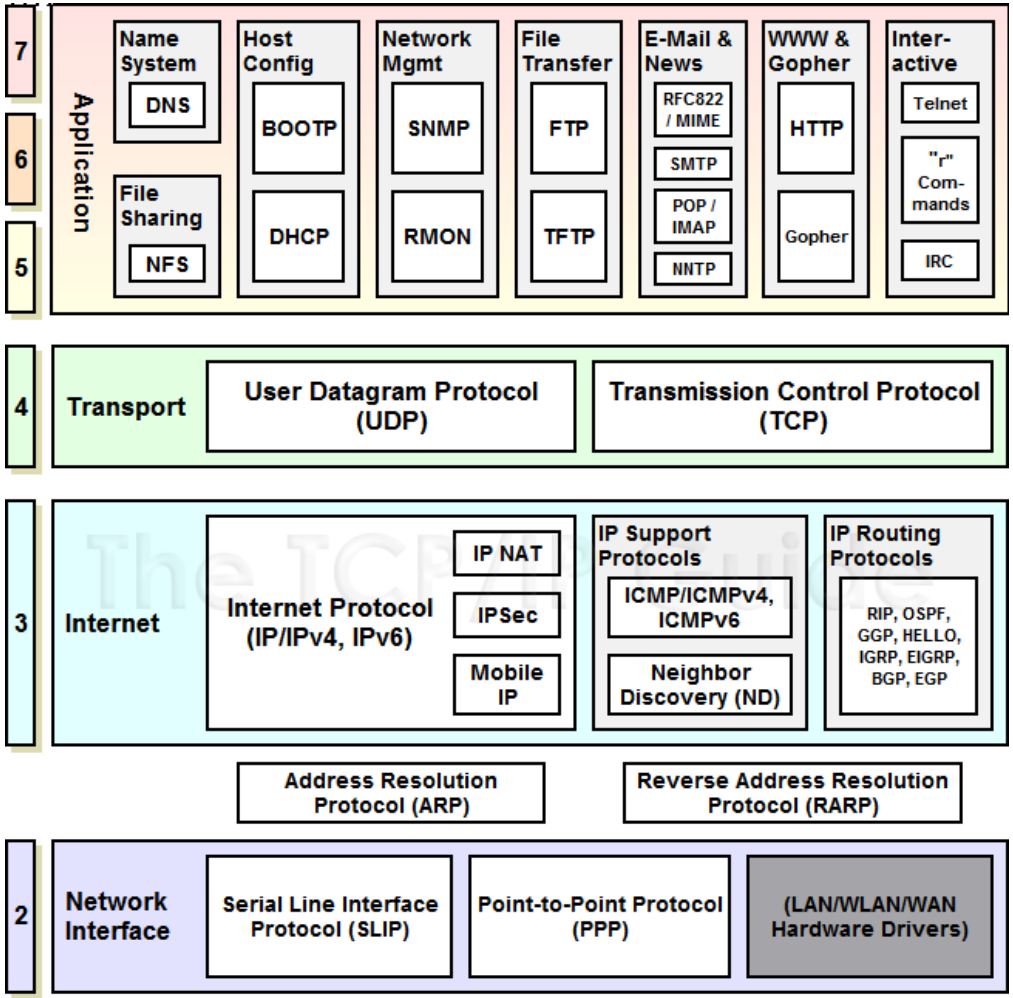
Yazılan programlar

- Farklı uç sistemlerde çalışır
- Ağ üzerinden haberleşir
- örnek, Web: Web server yazılımı browser yazılımı ile haberleşir

Ağ temel elemanlarına yönelik yazılım yapılmaz

- Network core cihazlar application layer'da çalışmaz
- Bu tasarım hızlı uygulama geliştirmeye izin verir

Uygulama Katmanı protokolleri



Uygulama katmanı protokolları

- **Bu protokollar (SMTP, TELNET, HTTP v.b) bir üstte çalışan kullanıcı programlarına hizmet verirler. Uygulama katmanı protokollarının herbiri, biri kullanıcı (Client- hizmet alan) diğeri sunucu (server- hizmet veren) da çalışmak üzere yapılandırılır.**
- **Web Browser, E-mail, Print Services, SIP, SSH and SCP, NFS, RTSP, Feed, XMPP, Whois, SMB; DNS; FTP; TFTP; BOOTP; SNMP;RLOGIN; SMTP; MIME; NFS; FINGER; TELNET; NCP; APPC; AFP; SMB**

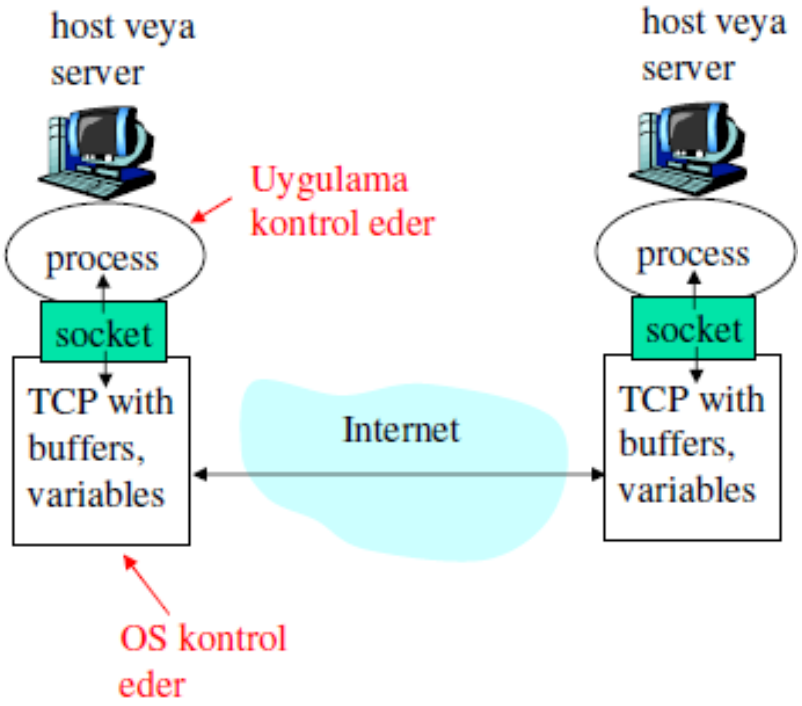
- **SMTP (Simple mail transport protocol):** Ağ içerisindeki kullanıcılar arasındaki e-mail alışveriş kurallarını düzenler.
- **SNMP(Simple network managment protocol):** Ağ içerisindeki ağ aktif cihazlarının yönetimi için kullanılan protokol.
- **TELNET :** Uzak bağlantı şeklidir. Sistem üzerindeki bir kullanıcının başka bir sisteme bağlanarak onun terminali gibi o sistemin kullanılmasını sağlar.
- **FTP (File Transfer Protocol):** Bir bilgisayardan başka bilgisayara dosya aktarımı için kullanılan protokol
- **HTTP (hyper Text Transfer Protocol):** WEB sahifelerinin alış-verişini sağlayan protokoldur.
- **DNS(Domain Name Server):** İnternet isimlerini IP noya çeviren protokoldur.

Uygulama Mimarileri

- Client-Server (İstemci –Sunucu)
- Peer-To-Peer (Eş düzey)
- Hibrid (C-S, P2P)

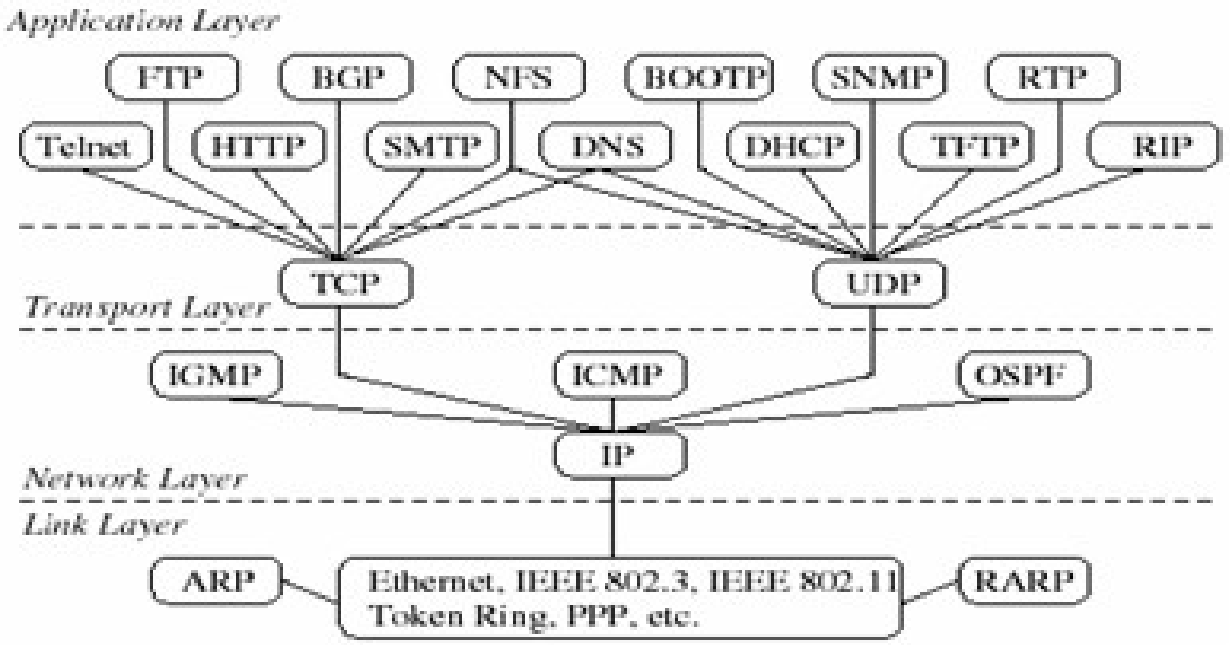
Soketler

- Process'ler kendi soketlerine mesaj gönderir veya alır
- soketler kapılara benzer
  - Gönderici process mesajı kapıdan dışarı gönderir
  - Gönderici process kapının diğer tarafındaki transport altyapısına güvenir

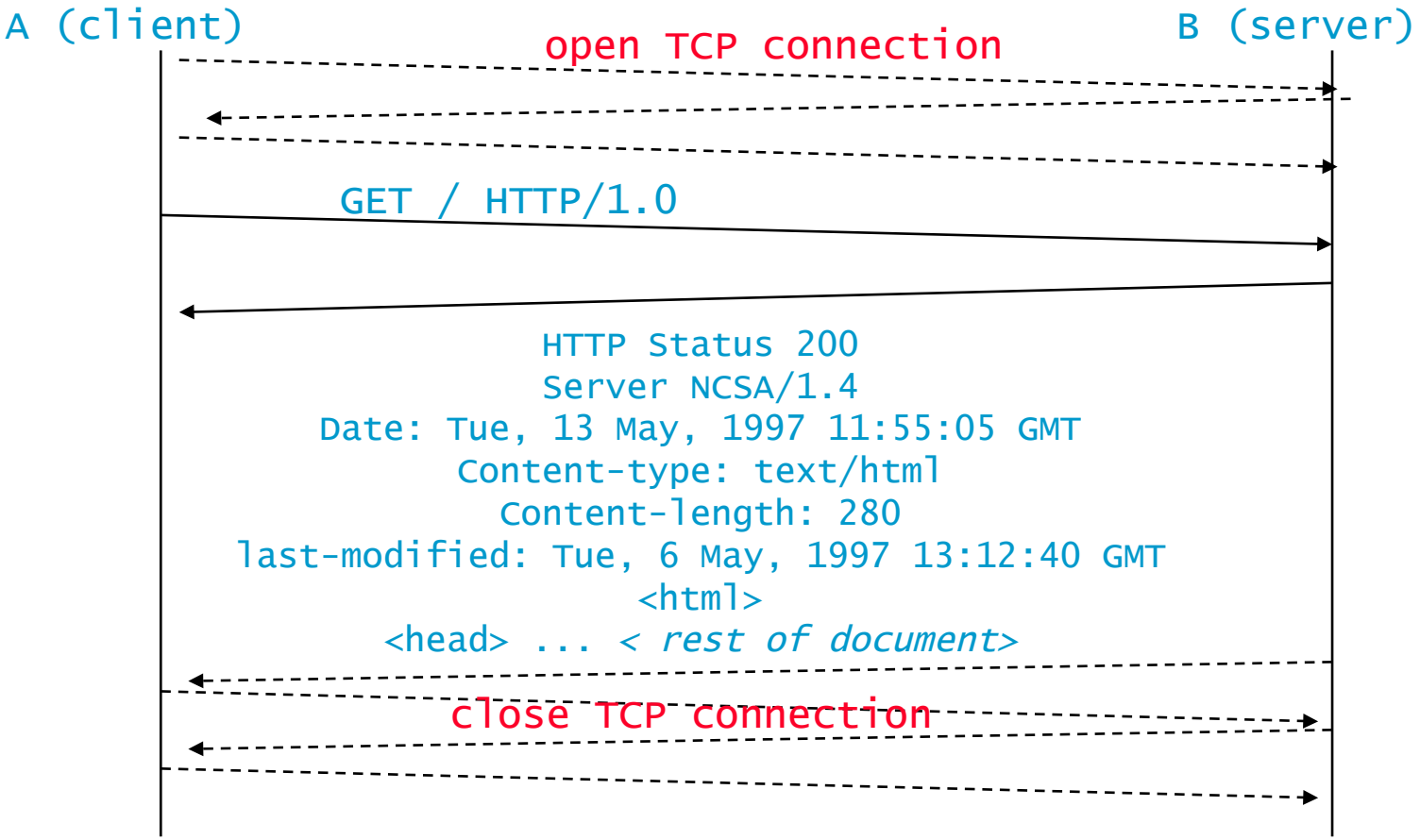


- API: (1) transport protokol seçer; (2) Parametre belirler

Protocols in Different Layers

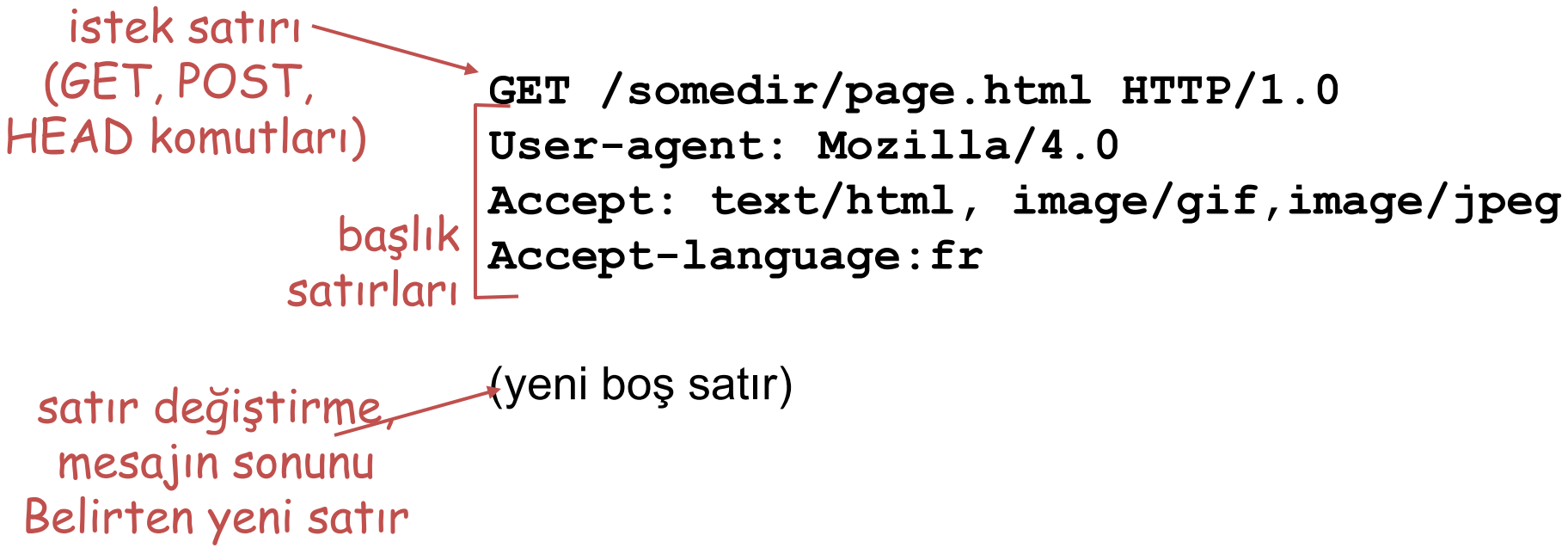


HTTP, TCP protokolunu kullanır.



http mesaj formatı

- iki tür http mesajı: *istek (request)*, cevap(response)
- http istek mesajı:
  - ASCII (okunabilir format)



http mesaj formatı: cevap

durum satırı (protokol durum kodu durum cümlesi)

başlık satırları

veri, örneğin, istenilen html dosyası

```
HTTP/1.0 200 OK
Connection: close
Date: Thu, 06 Aug 1998 12:00:15 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Mon, 22 Jun 1998 …...
Content-Length: 6821
Content-Type: text/html

data data data data data ...
```

Şimdiki örnekte de olmayan bir belge (web sayfası) için yapılan isteğe karşılık gönderilen sunucu cevabıdır.

HTTP/1.1 400 NOT FOUND
Date Wednesday, 28-Feb-07 19:51:28 GMT
Server: Apache/2.0

http cevap durum kodları

Sunucu-> kullanıcı cevap mesajının ilk satırında.

Bazı örnek kodlar:

200 OK

- istek başarılı, istenilen nesne bu mesajın sonrasında

301 Moved Permanently

- istenilen nesne yer değiştirdi, yeni konumu bu mesajın devamında belirtildi (Konum:)

400 Bad Request

- İstek mesajı servis sağlayıcı tarafından anlaşılmadı

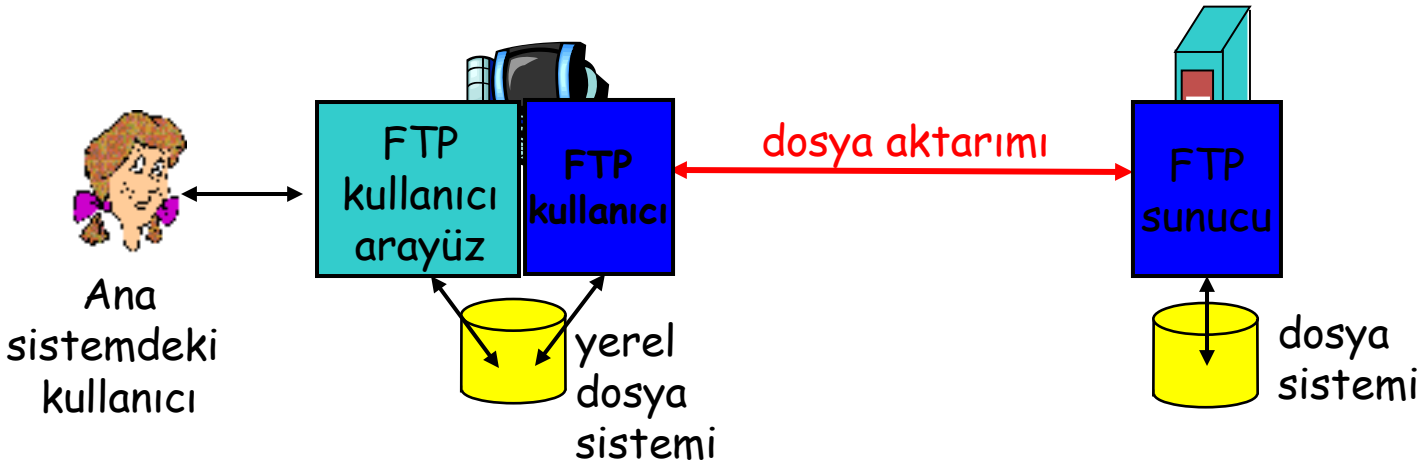
404 Not Found

- istenilen doküman bu servis sağlayıcıda bulunamadı

505 HTTP Version Not Supported

ftp: dosya transfer protokolu

ftp://sunucu_adi/dizin/dosya_adi
ftp://kullanici_adi@sunucu_adi/dizin/dosya_adi

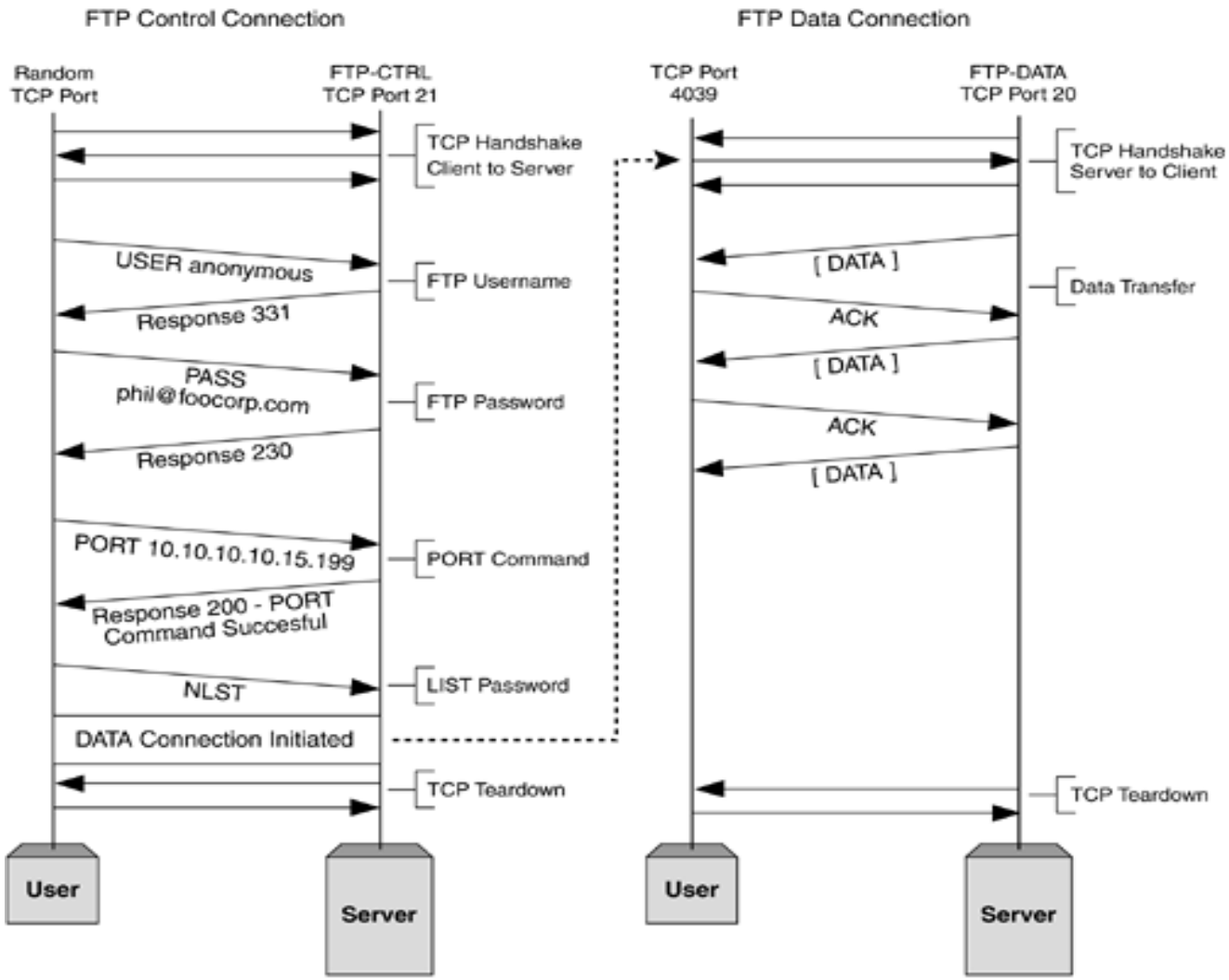


- Ana sisteme veya ana sistemden dosya aktarımı
- Kullanıcı/sunucu modeli
  - *kullanıcı:* transferi başlatan taraf (uzak dosya sistemine ya da sisteminden)
  - *sunucu:* uzaktaki ana sistem (remote host)
- ftp: RFC 959
- ftp sunucu: port 21

ftp: ayrık kontrol, veri bağlantıları

- ftp kullanıcısı ftp sunucusnu port 21 üzerinden aktarım protokolu olarak TCP'yi belirleyerek temasa geçer
- İki paralel TCP bağlantısı açılır:
  - kontrol: kullanıcı ve sunucu arasında komutlar, cevaplar değiştirilir.

    "band kontrolu dışında"
  - veri: sunucudan veya sunucuya dosya verileri
- ftp sunucusu "durumu" korur: kılavuz kütük (directory), önceden doğrulama (authentication)



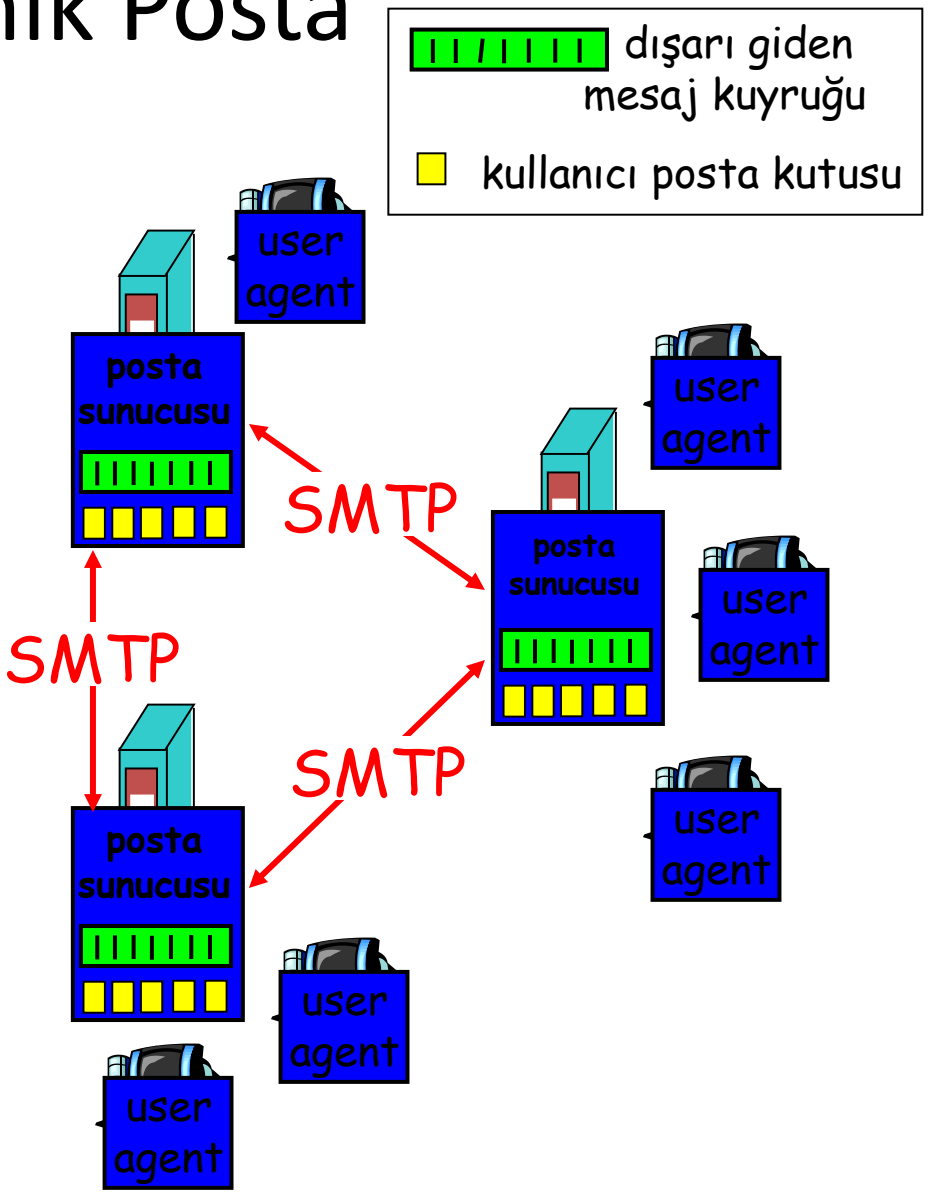
In an active FTP connection, the client will use the Control connection to tell the server, via a PORT command, which IP address and TCP port it should establish the Data connection to. The server then opens a Data connection to that IP address and port using the well-known Port 20 as the source.

Elektronik Posta

Üç temel bileşen:

- kullanıcılar
- posta sunucuları
- Basit posta akatarım (simple mail transfer) protokolu"

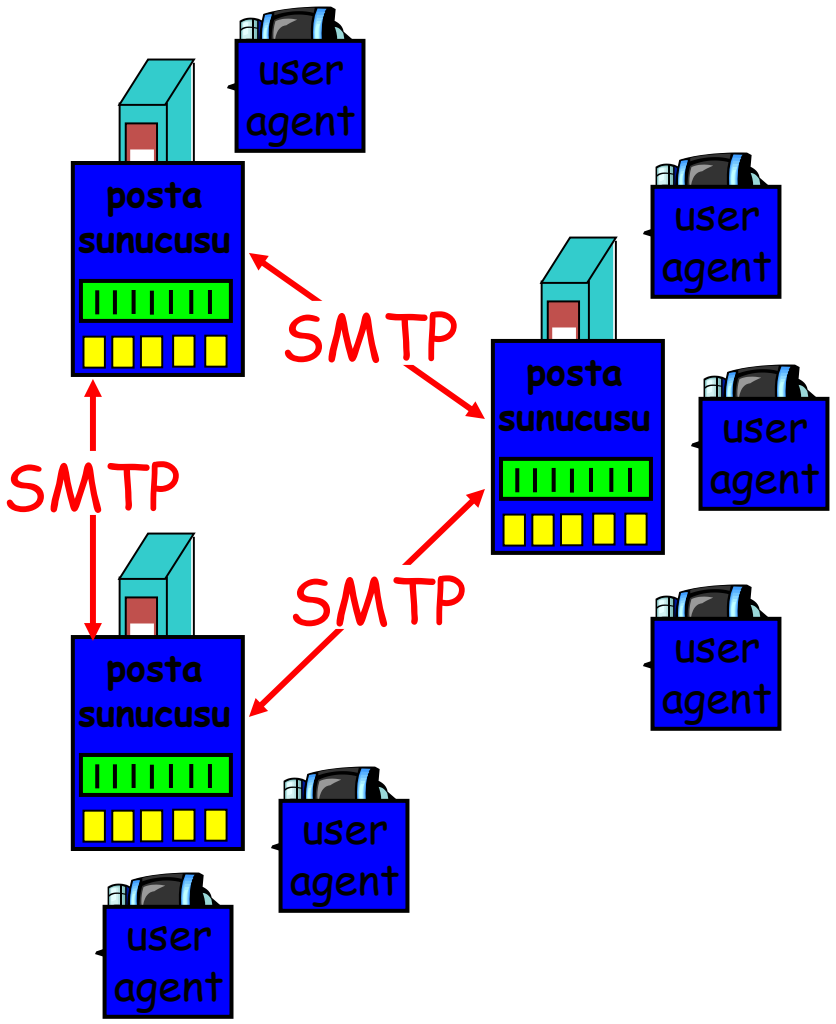
- User Agent (Kullanıcı arayüzü)
- "posta okuyucusu"
- Posta mesajlarını düzenleyen, yazan, okuyan
- örneğin, Eudora, Outlook, elm, Netscape Messenger
- giden, gelen mesajları sunucuda saklama



Elektronik Posta: posta sunucuları

Posta Sunucuları

- posta kutusu kullanıcı için (okunmak üzere) gelen mesajları bulundurur
- mesaj posta mesajları (gönderilmek üzere) kuyruğu
- smtp protokolu e-posta mesajları göndermek için posta servis sağlayıcıları arasında
  - *"kullanıcı":* gönderici posta sunucusu
  - "sunucu": posta alan sunucu



Elektronik Posta: smtp [RFC 821]

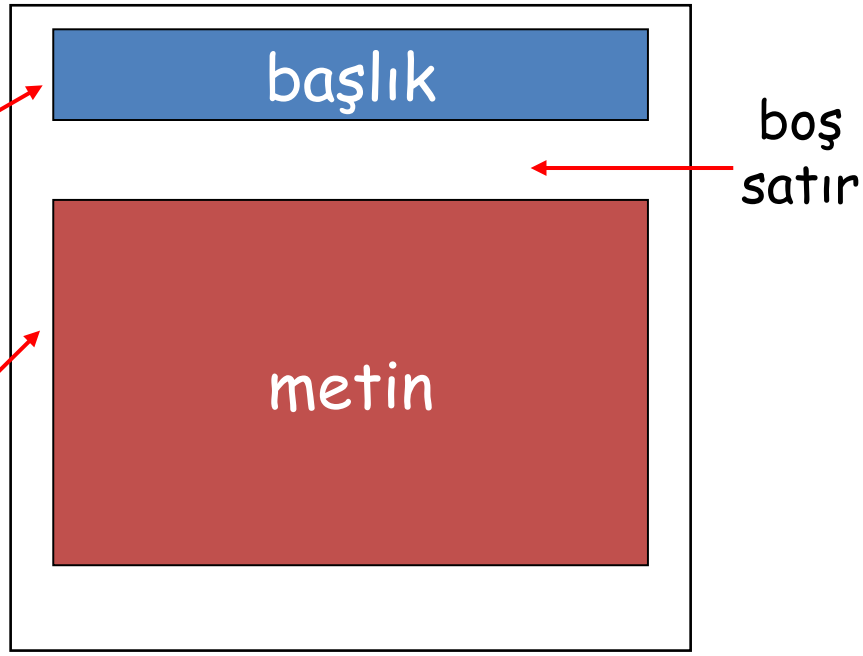
- Kullanıcıdan sunucuya eposta mesajlarını güvenilir bir şekilde aktarmak üzere tcp kullanılır, port 25
- doğrudan aktarım: gönderici sunucudan alıcı sunucuya
- Aktarımın üç aşaması
  - el sıkışması (handshaking, (greeting))
  - mesajların aktarılması
  - bitiş
- komut/cevap etkileşimi
  - komutlar: ASCII text
  - cevap: durum kodu ve cümle

Posta mesaj formatı

smtp: e-posta mesajlarini degistirmek uzere protokol

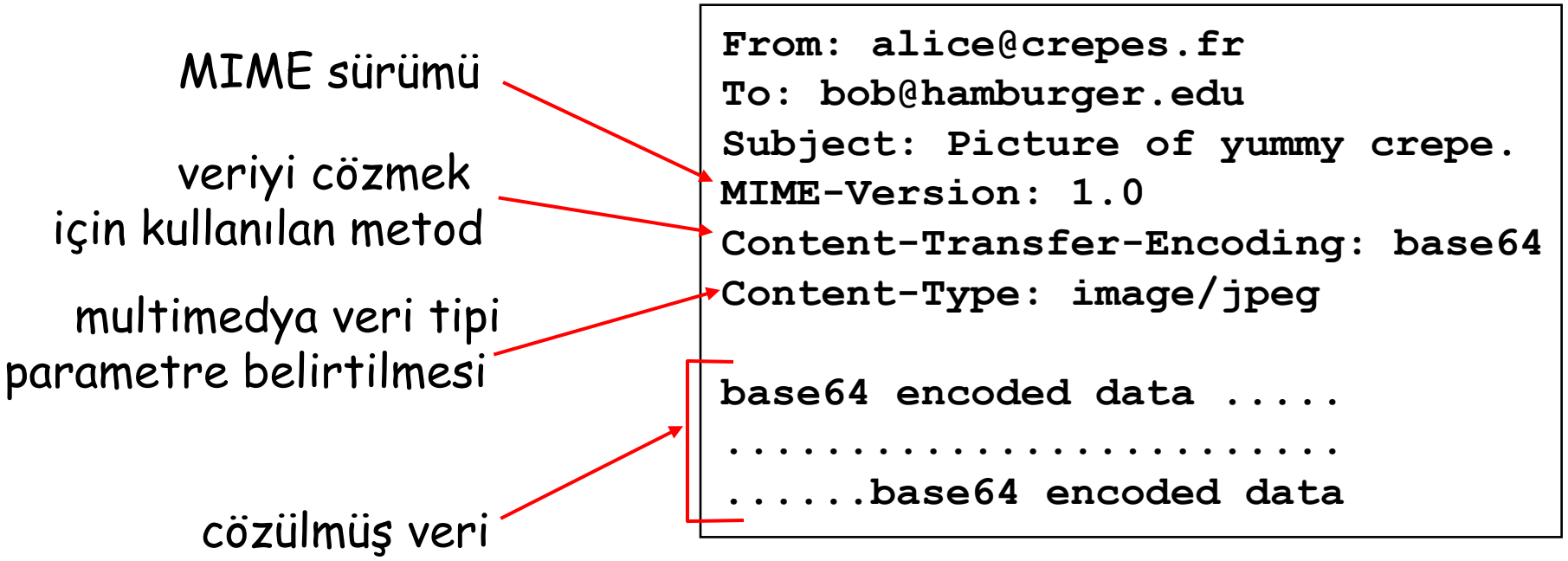
RFC 822: metin mesaj formati icin standart:

- Baslik satirlari, ornegin,
  - To:
  - From:
  - Subject:
  - *smtp komutlarindan farkli*!
- metin kismi
  - "mesaj", ASCII karakterleri kullanarak

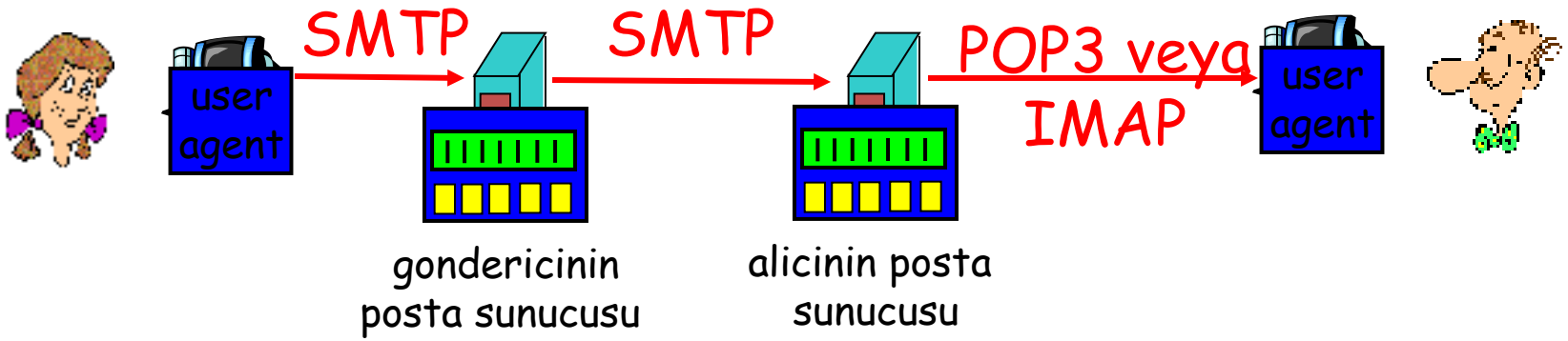


Mesaj formatı: multimedya uzantıları

- MIME: multimedia mail extension, RFC 2045, 2056
- Mesaj başlığındaki ilave satırlar MIME içerik bilgisini verir



Posta erişim protokolleri



- SMTP: alıcının sunucusuna teslimat/saklama
- Posta erişim protokolu: sunucudan yeniden alınması
  - POP: Post Office Protocol [RFC 1939]
    - yetkilendirme (agent <-->server) ve aliş (download)
  - IMAP: Internet Mail Access Protocol [RFC 1730]
    - daha fazla özellikler (daha fazla karışık)
    - sunucuda saklanan mesajlarin düzenlenmesi

DNS: Domain Name System

Kişiler: birçok tanımlayıcı:

- Sosyal Güvenlik Numarası, isim, pasaport #

- İnternet anasistemleri, yönlendiriciler(router):
  - IP adresi (32 bit) – veri akışını adreslendirmek için kullanılırlar
  - "isim", örneğin, gaia.cs.umass.edu – kişiler tarafından kullanılırlar

  Soru: IP adresleri ile isimler arasında dönüşüm ?

Domain Name System(Alan İsimlendirme Sistemi):

- *Dağıtılmış veri yapısı*

  birçok *isim sunucusunun* hierarşik (sıra) düzeninde uygulanırlar

- *Uygulama katmanı protoklou*

  ana sistem, yönlendiriciler, isim servis saglayıcıları isimleri *çözmek* üzere haberleşirler (adres/isim dönüşümü)
  - not: çekirdek İnternet fonksiyonu, uygulama katmanı protokolu olarak uygulanır
  - ağ "uç"'larında kompleks yapı

DNS isim servis sağlayıcıları

Neden DNS tek merkezli olamaz?

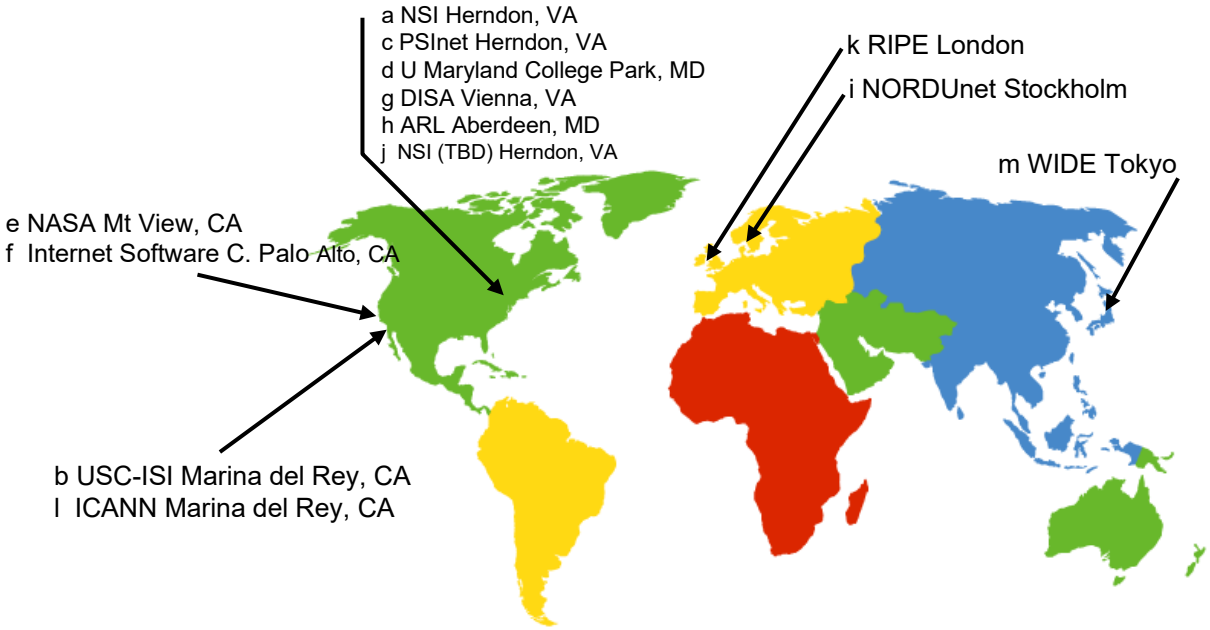
- tek noktada hata oluşması
- trafik hacimi
- uzak merkezi veri tabanı
- bakım

ölçeklendirme yapılamaz*!*

- servis sağlayıcılarının hepsi isim-IP adresleri dönüşümüne sahip değildirler
- yerel isim servis sağlayıcılar:
  - her ISP, şirket yerel *(default)* isim servis sağlayıcıya sahiptir
  - ana sistem DNS isteği ilk olarak yerel isim servis sağlayıcıya gider
- otoriter (authoritative) isim servis sağlayıcıları:
  - ana sistem için: bu ana sistemin IP adreslerini, isim bilgilerini saklar
  - bu ana sistem için isim/adres dönüşümünü gerçekler

DNS: Root isim servis sağlayıcıları

- isim/IP adres dönüşümünü çözemeyen yerel isim servis sağlayıcıları tarafından aranırlar
- root isim servis sağlayıcıları:
  - isim dönüşümü bilinmiyor ise (authoritative) isim servis sağlayıcılarına başvururlar
  - dönüşümü sağlar
  - yerel isim servis sağlayıcılarına dönüşümü gönderir



dünya genelinde 13 adet root isim servis sağlayıcı

TCP /IP V.4 ve OSI Uygulama katmanı Açıkları

- Katmanlı ağ modelinde, herbir katmandaki veri, doğrudan açık text formundadır. Yani xPDU ele geçirildiği anda içeriğinin rahatlıkla okunabildiği bir yapılanma sözkonusudur.
- xPDU ağda bulunduğu sürece değiştirilip değiştirilmediği, kimin gönderdiği veya kimin aldığı garantisi olmayan, gizliliğinin de tehdit altıda olduğu bir yapıdadır.
- Açık text yapısındaki bu xPDU'ların genellikle başlık yapısı değiştirilerek ataklar gerçekleştirilir. Bu durum uygulama katmanı mesajları içinde geçerlidir.
- Uygulama katmanının ve özellikle WEB uygulamalarının güvenlik açıkları; uygulama katmanı protokol açıklarıyla birlikte, uygulama yazılımları kodlama açıkları, sunucu, istemci ve iletişim ağı alt yapı (protokol açıkları da dahil) açıkları ile daha da artmaktadır.

İnternet'in kullanışlılığı ve karmaşıklığı, Web servis ve uygulamalarının kullanımının artmasıyla büyümekte ve ilgili güvenlik riskleri de orantılı olarak artmaktadır.

Bu tehditlerle mücadele etmek için, ağ güvenlik duvarı (Firewall), saldırı tespit sistemi (STS) veya saldırı önleme sistemi (SÖS) konuşlandırmanın, uygulama katmanına saldırılardan korumak için yeterli gelmeyeceği açıktır. Veya 3.katmanda paket filtrelemek te fazla önemli bir tedbir değildir. Çünkü uygulama katmanında biribirinden farklı uygulama yazılımları söz konusudur.

Open Web Application Security Project (OWASP) 'ın WEB uygulamaları için tanımladığı 10 adet açıklık ve tanımları tabloda verilmiştir.

TABLO I. OWASP İLK 10 AÇIKLIK, AÇIKLIK KAYNAKLARI VE ZARAR GÖREN TARAFLAR [22]

Sıra Nu.	Açıklıklar	Kaynak	Etkilenen
1	Enjeksiyon (Injection)	Uygulama	Sunucu
2	Kırık Kimlik Doğrulama ve Oturum Yönetimi (Broken Authentication and Session Management)	Uygulama	İstemci
3	Siteler Arası Betik Çalıştırma (Cross-Site Scripting -XSS)	Uygulama	Sunucu/ İstemci
4	Güvensiz Doğrudan Nesne Başvurusu (Insecure Direct Object References)	Uygulama	Sunucu
5	Güvenlik Yanlış Yapılandırma (Security Misconfiguration)	Sunucu	Sunucu
6	Hassas Veriyi Açıkta Bırakma (Sensitive Data Exposure)	Uygulama	Sunucu
7	İşlev Seviyesi Erişim Kontrolü Eksikliği (Missing Function Level Access Control)	Uygulama	Sunucu
8	Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery (CSRF))	İletişim Altyapısı	İstemci
9	Bilinen Açıklık Bileşenlerini Kullanma (Using Known Vulnerable Components)	Uygulama	Sunucu
10	Doğrulanmayan Yönlendirme ve İletme (Unvalidated Redirects and Forwards)	Uygulama	Sunucu/ İstemci

Uygulama katmanında (7.katman) en çok görülen Ataklar.

- **HTTP ilişkili ataklar**
- Viruses, Worms
- SQL Injection
- Cross Site Scripting (XSS)
- Malware (Trojans, Viruses, Worms, backdoors)

- **FTP ilişkili ataklar**
- Directory Traversal Attack :

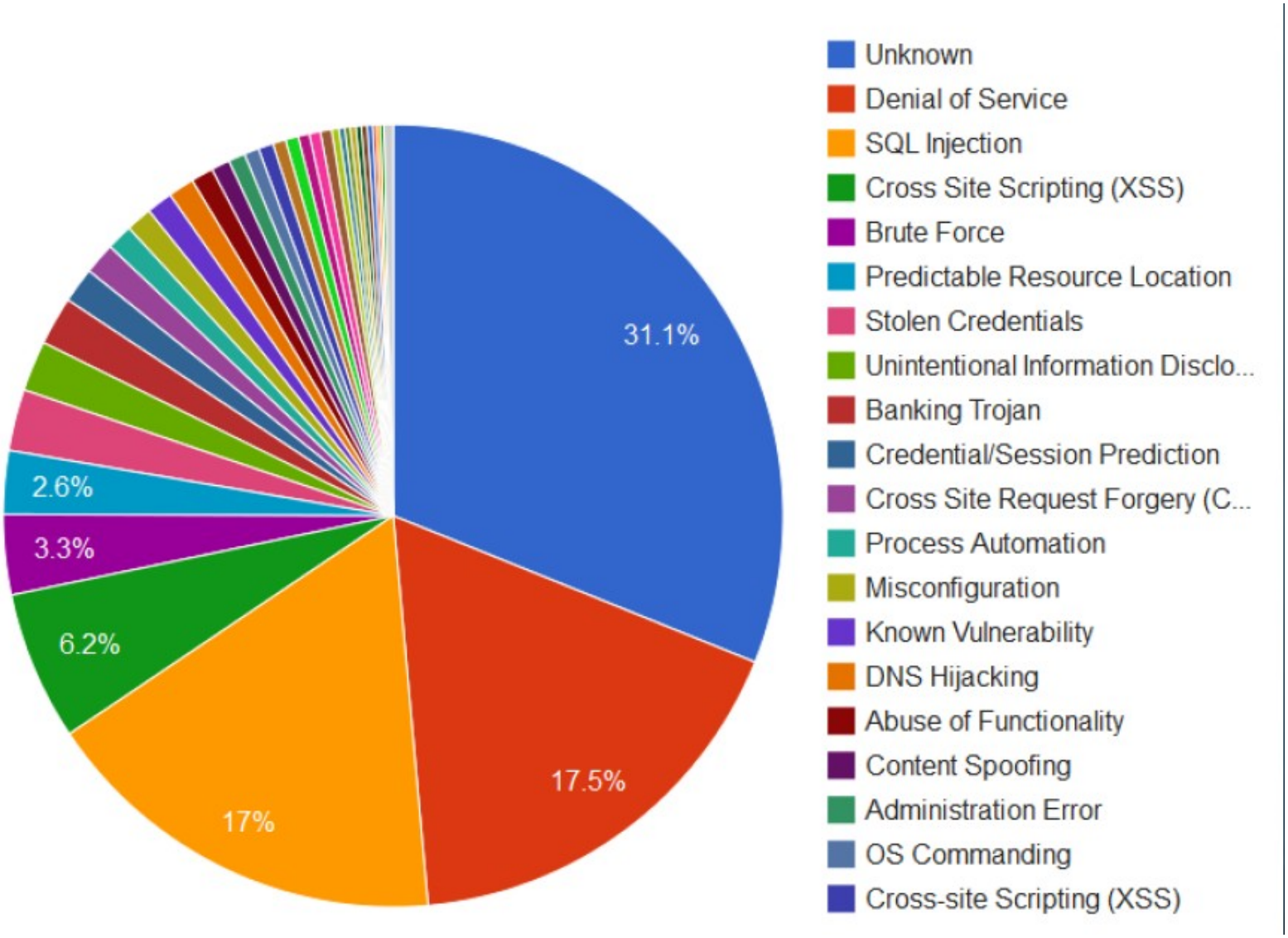
- **SMTP ilişkili ataklar**
- SMTP Worm
- Email spoofing
- IP Spoofing

- **DNS ilişkili ataklar**
- Man-in-the-Middle Attack
- Domain hijacking
- DNS flood attack
- Distributed Reflection Denial of Service (DRDoS)
- Cache poisoning

- **SNMP ilişkili ataklar**
- SNMP Flooding Attack
- Brute Force Attacks

DİKKAT!!! Uygulama katmanındaki bu atak tiplerinin öğrenilmesiyle ilgili bir hafta sonra verilecek ödevleri takip ediniz!!!!!

EN ÇOK KULLANILAN SALDIRI TİPLERİ (OWASP)



Uygulama Katmanı da dahil olmak üzere TCP/IP V.4 kümesinde, protokol açıklarından yararlanılarak her katmanda önemli saldırılar yapılabilir. Bu protokol açıklarını kapatmak için her katmanda tanımlanmış güvenlik protokolları mevcuttur. Bunlardan bazıları aşağıda verilmiş olup ilerleyen derslerde bu konularda açıklanacaktır.

- Application Layer (Uygulama Katmanı):
  - PGP (Pretty Good Privacy)
  - S/MIME (Secure/Multipurpose Internet Mail Extension)
  - S-HTTP (Secure-HTTP)
  - HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)
  - SET (Secure Electronic Transactions)
  - KERBEROS
- Transport Layer (Transport Katmanı):
  - SSL
  - TLS
- Network Layer (Netwok Katmanı):
  - IPSec
  - VPN
- Data Link Layer (Veri Bağı Katmanı):
  - PPTP
  - RADIUS
  - TACACS+