Module 4 - Day 1

Socket

Soket, TCP/IP'de, veri iletişimi için gereken iki bilgi olan IP adresi ve port numarasının yan yana yazılmasıyla oluşan iletişim kanalıdır. Örneğin, **192.168.1.1** makinesine **23** numaralı porttan yapılmış olan bir bağlantı **192.168.1.1:23** şeklinde yazılır.

Aynı zamanda, programlamada bir makineye bağlantı açıldığında buna "**soket açma**" denir. Bir soket açılınca, sistem programcıya IP adresi ve port numarasını verdiği için bu isimlendirme ortaya çıkmıştır.

Uygulama servisi olan bilgisayarlar başlangıçta soketleri dinlemeyi kurarlar. İletişim halindeki sistemler arasında bir bağlantı kurulduğunda, her bir bağlantı için bir soket oluşturulur. İşletim sistemi gelen IP paketlerini soket adresine göre uygun uygulama veya servise yönlendir

Python Socket Ornegi

Kaynak

echo-server.py

```
#!/usr/bin/env python3

import socket

HOST = '127.0.0.1'  # Standard loopback interface address (localhost)
PORT = 65432        # Port to listen on (non-privileged ports are > 1023)

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
    s.bind((HOST, PORT))
    s.listen()
    conn, addr = s.accept()
    with conn:
        print('Connected by', addr)
        while True:
            data = conn.recv(1024)
            if not data:
                break
            conn.sendall(data)
```

echo-client.py

```
#!/usr/bin/env python3

import socket

HOST = '127.0.0.1'  # The server's hostname or IP address
PORT = 65432        # The port used by the server

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
    s.connect((HOST, PORT))
    s.sendall(b'Hello, world')
    data = s.recv(1024)

print('Received', repr(data))
```

FTP (File Transfer Protocol)

Kaynak: https://tr.wikipedia.org/wiki/Dosya_aktarım_iletişim_kuralı

Dosya aktarım iletişim kuralı, (İngilizce: **F**ile **T**ransfer **P**rotocol; **FTP**), bir veri yığınının - ASCII, EBCDIC, ve binary- bir uç aygıttan diğerine iletimi için kullanılmaktadır.

Bir dosyayı FTP kullanarak başka bir TCP/IP ağı üzerindeki kullanıcıya yollamak için o ağdaki bilgisayarda geçerli bir kullanıcı ismi ve şifresi gerekmektedir. Birçok FTP sunucusu, kullanıcı ismi ve parola olmadan erişim için "anonim FTP" (anonymous FTP) desteği verir, bu kullanım için kullanıcı adı olarak anonymous parola olarak ise bir e-mail adresi girilmesi gerekmektedir (Internet Explorer, e-mail olarak IEuser@ girer).

FTP, dosya transferi ve komut transferi için değişik portlar kullanır. Varsayılan konfigürasyonda, komut transferi (yani sisteme giriş, klasör değiştirme, dosya adı değiştirme veya "dosya yolluyorum" komutları) için kullanılan port numarası 21'dir. Dosyalar indirilir veya gönderilirken ise o an boş olan bir port numarası kullanılır.

FTP RFC959 → https://tools.ietf.org/html/rfc959

OSI Modeli

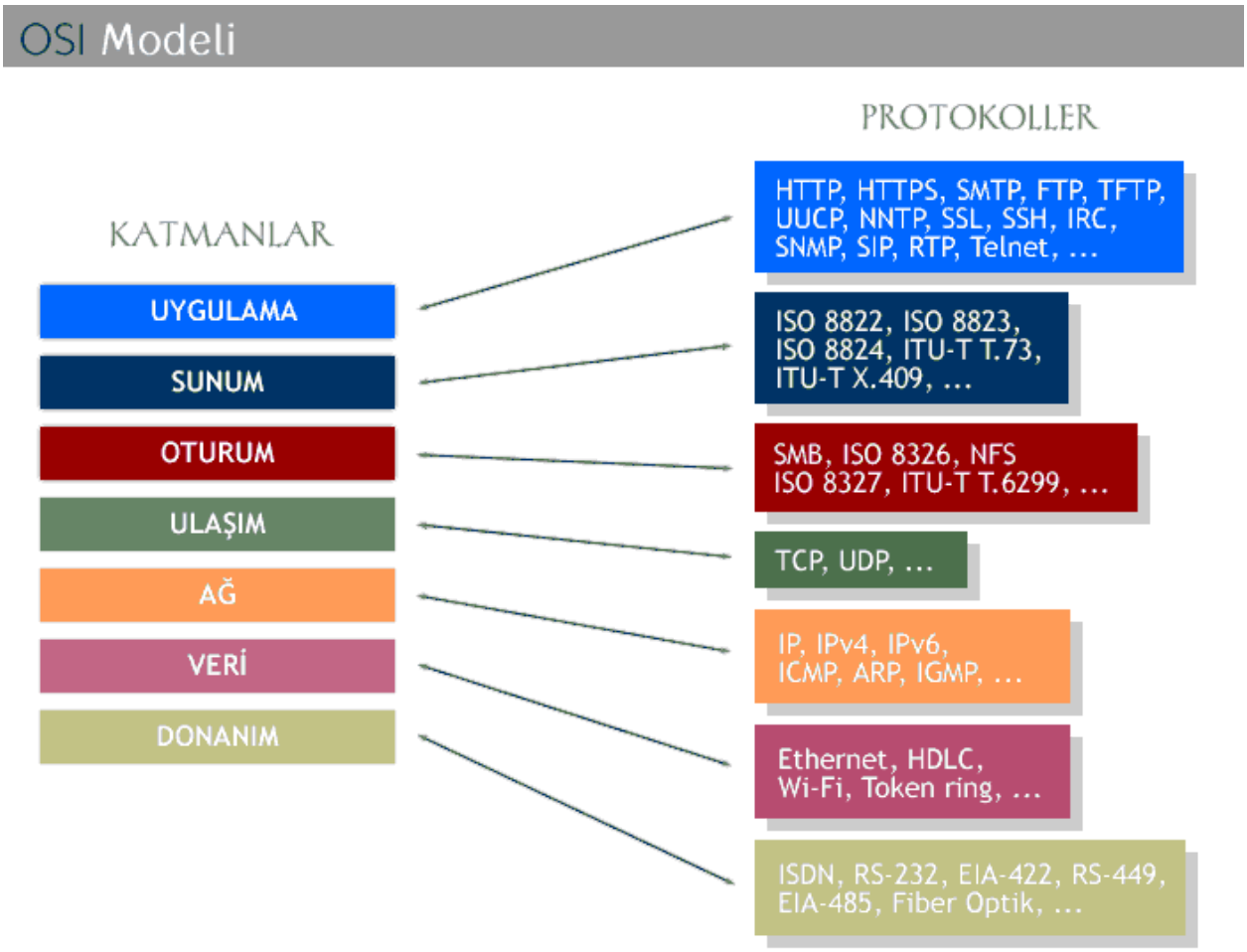
Kaynak: https://tr.wikipedia.org/wiki/OSI_modeli

Open Systems Interconnection (**OSI**) modeli ISO (International Organization for Standardization) tarafından geliştirimiştir. Bu modelle, ağ farkındalığına sahip cihazlarda çalışan uygulamaların birbirleriyle nasıl iletişim kuracakları tanımlanır.[1]

İlk OSI standartları 1970'lerin sonlarında ve 1980'lerin başlarında ISO'nun TC 97 (Technical Committee 97), Enformasyon İşlemesi tarafından ortaya çıkartılmıştır.[2] ISO, son OSI standardını 1984'te çıkartmıştır.[3] Bu model kısa sürede kabul görerek yaygınlaşmış ve ağ işlemleri için bir kılavuz olmuştur.

Open Systems Interconnection (**OSI**) modeli ISO (International Organization for Standardization) tarafından geliştirimiştir. Bu modelle, ağ farkındalığına sahip cihazlarda çalışan uygulamaların birbirleriyle nasıl iletişim kuracakları tanımlanır.[1]

İlk OSI standartları 1970'lerin sonlarında ve 1980'lerin başlarında ISO'nun TC 97 (Technical Committee 97), Enformasyon İşlemesi tarafından ortaya çıkartılmıştır.[2] ISO, son OSI standardını 1984'te çıkartmıştır.[3] Bu model kısa sürede kabul görerek yaygınlaşmış ve ağ işlemleri için bir kılavuz olmuştur.



IETF(Internet Engineering Task Force)

Kaynak: https://tr.wikipedia.org/wiki/İnternet_Mühendisliği_Görev_Gücü

İnternet Mühendisliği Görev Grubu (İng. İngilizce: Internet Engineering Task Force (İngilizce: IETF), İnternet protokollerini geliştiren ve standartlaştıran, resmî statüsü olmayan bir gruptur. IETF'nin çalışmaları ve ürettiği dokümanlar İnternet üzerinden herkese açıktır. Çalışma gruplarına ve toplantılarına katılım için herhangi bir kısıtlama bulunmamaktadır. Toplantılar, genellikle İnternet üzerinden tartışma grupları aracılığıyla sanal olarak yapılmaktadır.

> **RFC Yorumlar İçin Talep** (Orijinal adı: Request For Comments, RFC), TCP/IP nin tanımlanmasında kullanılan standart numaralara sahip dokümanlardır.

HTTP RFC2616 → https://tools.ietf.org/html/rfc2616

IP (Internet Protocol)

Kaynak: https://tr.wikipedia.org/wiki/Internet_Protocol

Internet Protocol (IP) ağ sınırları boyunca datagramların geçişi için internet protokolü takımında temel iletişim protokolüdür. Yönlendirme işlevi sayesinde internetin çalışmasını sağlamaktadır. IP, paket teslim görevini paket başlıklarındaki IP adreslerine dayalı olarak kaynak adresten hedef adrese doğru gerçekleştirir. Bu amaçla, IP veri teslim edilecek kapsülleyen bir paket yapıları tanımlamaktadır. Aynı zamanda adresleme yöntemlerini tanımlayan bu metot kaynak ve hedef bilgileri ile diyagramı etiketlemek için kullanılır. IP, 1974 yılında Vint Cerf ve Bob Kahn tarafından orijinal iletim kontrol programında bağlantısız bir datagram hizmeti olarak tanıtıldı. İnternet protokolü paketi bu nedenle sık sık TCP/IP gibi ifade edilir. IP'nin ilk büyük versiyonu İnternet Protokolü Sürüm 4'tür. IPv4 internette baskın olan bir protokoldür. Protokolün halefi ise İnternet Protokolü Sürüm 6 (IPv6)'dır.

URL RFC1738 → https://tools.ietf.org/html/rfc1738

Further Reading

40 maps that explain the internet → https://www.vox.com/a/internet-maps

Türkiye' de İnternet' in 25. Yılı Belgeseli → https://www.youtube.com/watch?v=AEXWn-NsmXY

TCP (Transmission Control Protocol)

Kaynak: https://tr.wikipedia.org/wiki/TCP

TCP (Transmission Control Protocol), TCP/IP protokol takımının aktarım katmanı protokollerinden birisidir. Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde kayıpsız veri gönderimi sağlayabilmek için TCP protokolü yazılmıştır. HTTP, HTTPS, POP3, SSH, SMTP, Telnet ve FTP gibi internet'in kullanıcı açısından en popüler protokollerinin veri iletimi TCP vasıtasıyla yapılır.

SSH Güvenli Kabuk

Güvenli Kabuk (**SSH**), ağ hizmetlerinin güvenli olmayan bir ağ üzerinde güvenli şekilde çalıştırılması için kullanılan bir kriptografik ağ protokolüdür.[1] En iyi bilinen örnek uygulaması bilgisayar sistemlerine uzaktan oturum açmak için olandır.

SSH, bir SSH istemcisini bir SSH sunucusuna bağlayarak istemci-sunucu mimarisi çerçevesinde güvenli olmayan bir ağ üzerinde güvenli kanal sağlar.[2] Yaygın uygulamalar arasında uzaktan komut satırı girişi ve uzaktan komut çalıştırma bulunur, ama herhangi bir ağ hizmeti de SSH ile güvenceye alınabilir. Protokol belirtimi SSH-1 ve SSH-2 olarak adlandırılan iki ana sürüm arasında ayrım yapar

```
# Asagidaki sekilde baglanti saglanabilir

SSH root@ip
```

SFTP

Secure FTP (Güvenli Dosya Taşıma Protokolü), yani SFTP, SSH kullanarak dosya transferi yapan bir dosya aktarım protokolüdür. SSH'ın sağladığı güvenlik özellikleri, FTP'den farklı olarak SFTP'yi güvenli hale getirir. FTP'nin RSA ile güçlendirilmiş halidir. TCP üzerinden çalışır.

SSH ile SFTP Kullanımı

SFTP ile dosya transferi yapabilmek için bir SFTP istemcisine sahip olmak gereklidir. Neredeyse bütün Linux dağıtımlarında bir SFTP istemcisi ön tanımlı olarak bulunur. Windows işletim sistemlerinde bir SFTP istemcisi edinerek kurmak gerekir.

SFTP Komutları

- Host ile bağlantı kurma: $sftp

  host_adi

- Oturum açma: $sftp

  kullanici_adi@host_adi

- help: Yardım komutudur. sftp ile kullanılabilecek komutların ve bu komutların işlevlerinin listesini verir.

- put: Host bilgisayara dosya kopyalar.

sftp> put kaynak_dosya_konumu (hedef_konum)

- get: Host bilgisayardan istemci bilgisayara dosya kopyalar.

sftp> get kaynak_dosya_konumu (hedef_konum)

- cd: Host bilgisayarda dizin değiştirme komutu. (Linux işletim sistemindeki cd komutunun aynısı.)
- lcd: İstemci bilgisayarda dizin değiştirme komutu.
- rm: Host bilgisayarda dosya silme.
- rmdir: Host bilgisayarda dizin silme.
- chmod: Dosyalara ait kullanıcı izinlerini değiştirmenizi sağlar.

sftp> chmod izin_kodu dosya_konumu

- ls: Host bilgisayarda dizin içeriğini listeleme.
- lls: İstemci bilgisayarda dizin içeriğini listeleme.
- rename: Host bilgisayarda dosya adı değiştirme.

sftp> rename eski_isim yeni_isim

- mkdir: Host bilgisayarda dizin oluşturma.
- lmkdir: İstemci bilgisayada dizin oluşturma.
- Oturum kapatma ve SFTP'den çıkma:sftp> exit sftp> quit sftp>

SCP

Kaynak: https://www.hosting.com.tr/bilgi-bankasi/scp-nedir/

SCP, açılımı Secure Copy Protocol olan ve Güvenli Kopyalama Protokolü anlamına gelen, iki farklı Linux tabanlı bilgisayar veya sunucu arasındaki dosya aktarım aracıdır. FTP alternatifi olarak düşünülebilir. Secure Copy , SSH Protokolünü kullandığı için güvenli bağlantı sağlamaktadır

SCP Nasıl Kurulur?

Linux tabanlı cihazlarda SCP ekli olarak gelmemektedir. Sadece OpenSSH-Client'in kurulu olduğu sistemlerde SCP eklidir.

Aşağıdaki komutlarla SCP Arasını kolayca kurabilirsiniz.

```
root# apt-get install openssh-client -y  (#Debian/Ubuntu)

root# yum install openssh-client -y    (#RHEL/CentOS/Fedora)
```

SCP Parameterleri Nelerdir?

- p : Hedef dizindeki port bilgilerini girmek için kullanılır.
- q : Transer sırasında gösterilen yüzdelik oranı kapatır ancak işlemi sonlandırmaz, sadece arayüzde göstermez.
- r : Dosyaları kopyalamak için kullanılır.
- C : Transfer sırasında dosyaları sıkıştırarak kopyalama hızını artırır.
- i : Ortak anahtar kimlik doğrulaması veya özel anahtar (ssh key) dosyasını kullanmak için kullanılır.
- l : Bant genişliğini (Bandwidth) limitlendirmek için kullanılabilir. Kbit/s.
- v : Hata ayıklama raporlarını görüntülemek için kullanılır.
- c : Veri transferi sırasında şifreleme yöntemini "-c blowfish cipher" şeklinde değiştirir.

SCP ile Dosya Transferi Nasıl Yapılır?

SCP ile dosya transfer etmek çok kolay! Birkaç örnekle transferin nasıl gerçekleştiğini anlatacağım.

Alt örnekteki komutu kullanarak hedef bilgisayar veya sunucudaki **/bilgi** dizini içerisine **mesaj.txt** adlı dosyayı transfer edebiliriz. Komutu kullandıktan sonra karşı bilgisayar veya sunucunun şifresini isteyecektir.

```
root# scp mesaj.txt root@85.66.123.145:/bilgi/
```

Alt örnekteki komutu kullanarak hedef bilgisayar veya sunucudaki **/bilgi/mesaj.txt** adlı dosyayı bulunduğumuz dizine transfer edebiliriz.

```
root# scp root@85.66.123.145:/bilgi/mesaj.txt  .
```

Alt örnekte hedef bilgisayar veya sunucudaki **/bilgi/mesaj.txt** adlı dosyayı, kendi bilgisayar veya sunucumuzdaki **/bilgi/admin/** dizinine kopyalamak.

root# `scp root@5.5.5.5.5:/bilgi/mesaj.txt /bilgi/admin/`

SOAP

Kaynak: https://tr.wikipedia.org/wiki/SOAP

SOAP (Simple Object Access Protocol - Basit Nesne Erişim Protokolü), Service-oriented Architecture felsefesini pratiğe uyarlayan iki interface'den biridir. Üzerinde bulunan Universal Description Discovery and Integration (UDDI) ile birlikte hizmet yönelimli mimarinin pratikte kullanılmasını mümkün kılar.

Bir SOAP mesajının yapısı

- **Envelope:** Bütün SOAP mesajlarının içinde olduğu elemandır. SOAP mesajına ilişkin XML belgesinin root elemanı olmak zorundadır. Envelope elemanı içinde Body veya Header gibi elemanlar bulunur. Envelope elemanının içinde her zaman bir Body elemanı vardır fakat Header elemanı olmak zorunda değildir. SOAP mimarisine göre eğer Envelope elemanı içinde Header elemanı varsa bu eleman Envelope elemanının içindeki ilk eleman olmalıdır. Soap kullanan mimarilerde kesinlikle erişim protokolü olarak TCP kullanılmalıdır
- **Header :** SOAP mesajlarındaki Header elemanını HTML standartlarında bulunan <Head></Head> etiketlerine benzetebiliriz. Header bölümü metot çağrımı ile doğrudan ilişkili değildir. Header bölümü ile meta-data dediğimizi bilgiler gönderilir.
- **Body:** Body elemanı SOAP mesajının en önemli kısmını oluşturur. Body bölümünde web metodunun adı ve metodun parametrik bilgileri XML formatında gönderilir. Cevap mesajında ise metodun geri dönüş değeri Body bölgesine eklenir. Metodun parametrik yapısının bu şekilde XML formatında

yazılmasına SOAP Serialization denir. Son olarak hata mesajlarında ise Body bölümünde hatanın adı ve tanımı gibi bilgiler bulunur.

Keywords, Tools:

- rsync
- WSDL dosyasi
- jq json
- json blob.com
- telnet
- tracerout

  https://curl.trillworks.com/ curl converter