TEMEL KAVRAMLAR

Giriş

Web güvenliği için 3 ana kural mevcuttur.Bütünlük,Gizlilik,Erişebilirlik gereklidir.

ŞİFRELEME

Charset:HTML karakter seti, web tarayıcıların html sayfasındaki karakterlerin ne olduğunu anlaması içindir. Yani bizim hangi karakteri kullanacağımızı belirtiyoruz. Bu sayede tarayıcılar anlıyor.

CİPHER: Bir text'i şifreli metne çeviren yapıya cipher denilir.

HASH

Hash: Bir belge/metinin bütünlüğünü kontrol eden yapıdır.Md5 ve sha512 -sha:x gibi hash tiplerdir.

Salting

Ek karakter eklenip hashlenmesine salting denilir.Örneğin bir username'nin sonuna ek karakter ekleyerek saldırganının şifreyi alması engellenir.

HASH KIRMA YÖNTEMLERİ

Rainbow table,john the ripper ,hashcat araçlar kullanılıyor.

ENCODE

Verinin farklı bir biçime dönüştürülmesidir.Örneğin:Metni bir charsetten başka bir charsete dönüştürülmesidir.Örneğin binarydan asciiye çevrilmesidir.

DECODE

Encode'un tam tersidir.Çözümleme işidir.

ENCRYPTİNG

Şimdi ise şifreleme kısmına gelelim. 2 farklı şifreleme algoritmaları vardır.

SİMETRİK

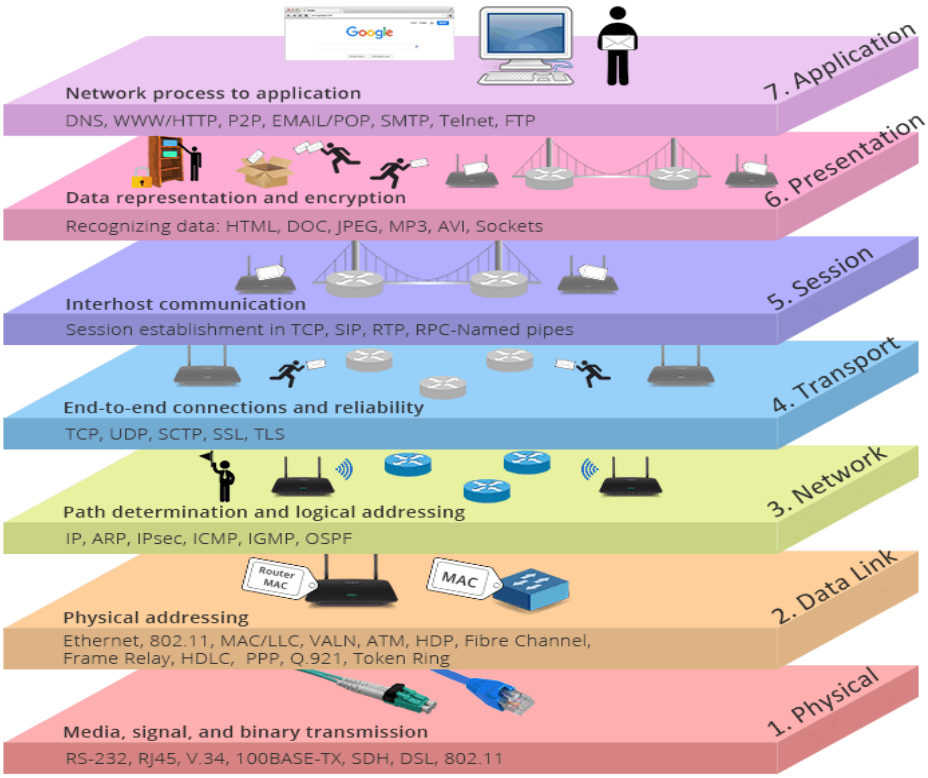
Hem şifreleme ,hem deşifreleme için aynı anahtar kullanılıyorsa buna simetrik şifreleme denir. CEASER,AES256,DES,RC5 gibi algoritmalar kullanılır.

ASİMETRİK

Şifreleme ve deşifreleme için farklı anahtar kullanılıyor,bir açık,bir kapalı anahtar kullanılır.

RSA256,PGP,SHA,MD5 gibi algoritmalar kullanılır.En temel algoritma ise diff hellmandır.

OSİ KATMANLARI



TCP-IP/UDP

Bağlantı protokolleri arasında farklara değinelim.

TCP/IP: Bir bağlantıda gönderilen verinin karşı tarafa ulaşıp ulaşmadığını kontrol eder.

TLS handshake, bir istemci ile sunucunun TLS kullanarak güvenli bir bağlantı kurma işlemidir. TLS handshake sırasında, güvenli bir bağlantı kurmak için istemci ve sunucu anahtarları ve sertifikaları değiş tokuş eder.

UDP:TCP'ye göre daha hızlıdır fakat güvenli değildir. Veri ismine datagram denilir. Datagramın segmentten farkı ise içerisinde sıra numarasının bulunmamasıdır.

Websocket açarken veya video vs atarken udp kullanılır.

Ek kaynak:https://www.karel.com.tr/bilgi/tcp-ve-udp-arasindaki-farklar-nedir

STANDART UDP ALT PROTOKOLLERİ VE PORTLARI

RDP

RDP "Remote Desktop Connection" Windows çalıştıran bir bilgisayara, Uzak Masaüstü Bağlantısı kullanarak, aynı ağa veya İnternet'e bağlı olan ve Windows çalıştıran başka bir bilgisayardan erişebilirsiniz. Örneğin, işyerindeki bilgisayarınızın tüm programlarını, dosyalarını ve ağ kaynaklarını evinizdeki bilgisayarınızdan işyerindeymiş gibi kullanabilirsiniz

Rdp port 3389 dir.

VNC

Bir ağ sunucusu üzerinde çalışan grafik arabirimli uygulamalara, başka bir ağ üzerindeki bilgisayardan erişerek bu uygulamaların kullanabilmesini ve yönetilebilmesini sağlar.

Default port 5900 dir.

STANDART TCP/IP ALT PROTOKOLLERİ VE PORTLARI

SSH

SSH, veya Secure Shell, kullanıcılara sunucularını internet üzerinden kontrol etmesini ve düzenlemesini sağlayan uzak yönetim protokolüdür.
Default portu 22 dir.

SMB

Server Message Block(Sunucu İleti Bloğu), server-client arasındaki iletişimi sağlayan bir ağ protokolüdür. SMB protokolü, Windows sistemlerinin 139 ve 445 portlarını kullanarak, paylaşılan dosyalara erişimi, ağlar, yazıcılar ve çeşitli bağlantıları sağlar. Bu bağlantıların yanında oplock, dosya ve kayıt kitleme, dosya ve dizin değişikliği gibi işlemler de SMB üzerinden gerçekleşmektedir.

Default port 445 dir.

FTP

Ftp,açılımı File Transfer Protocol olan FTP'nin Türkçe karşılığı Dosya Transfer Protokolü'dür. İsminden de anlaşılabileceği gibi internete bağlı iki bilgisayar arasında dosya transferini sağlayan bir protokol ve bu işleme hizmet eden uygulamaya verilen isimdir.Default port 21 dir.

STMP

SMTP (Simple Mail Transfer Protocol), bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür.

Default port 25 dir.

POP3

POP3 (Post Office Protocol 3 - Postane Protokolü 3), OSI referans modelinin uygulama katmanında çalışan bir E-posta iletişim protokolüdür.

Default port 110 dir.

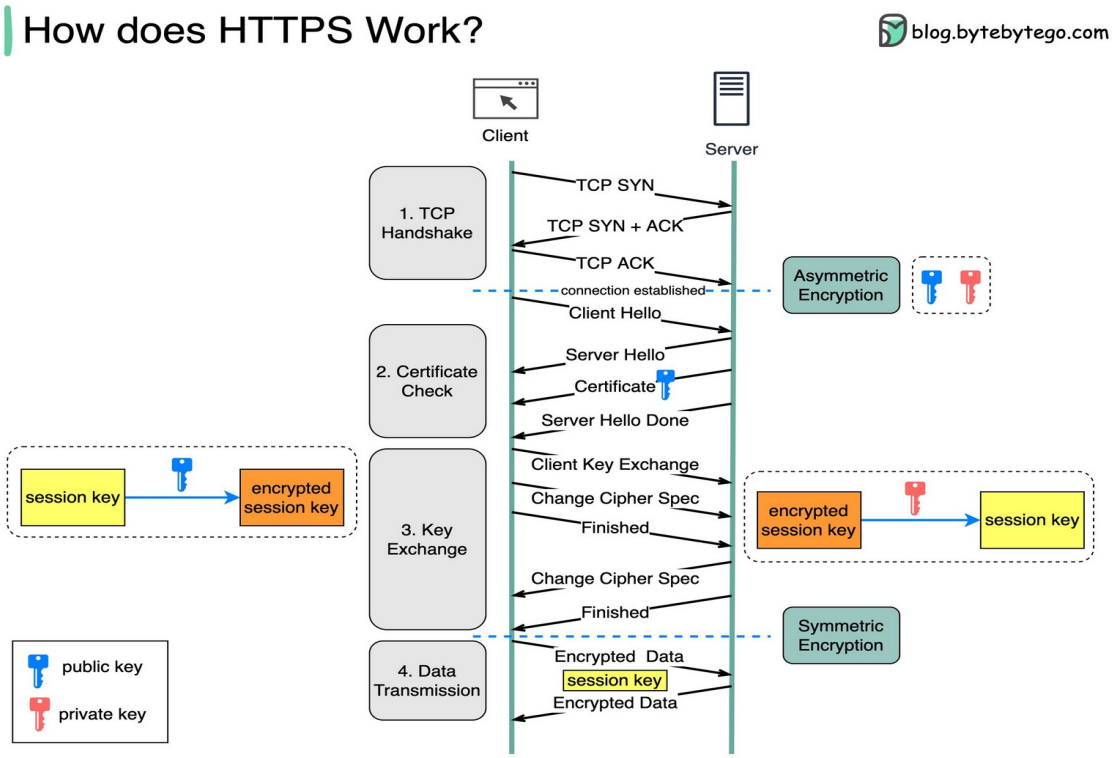
--HTTP--

Bilginin uygulama seviyesinde dağıtılmasını sağlayan protokoldür.Protokol sunucu ve istemci arasında köprü görevi görür. Veriyi açık şekilde gönderir.

Default portu 80 dir.

--HTTPS--

Https'in httpden en büyük farkı veriyi şifreliyor olmasıdır.SSL sertifikası sayesinde gönderilen veri şifrelenir.



Not:session key-master keyde deniliyor.

Https'de Client-Server ile gönderilirken,cypherset üzerinden en güçlü algoritma seçer.

CLİENT | Server

X | a

Y | z

Z | b

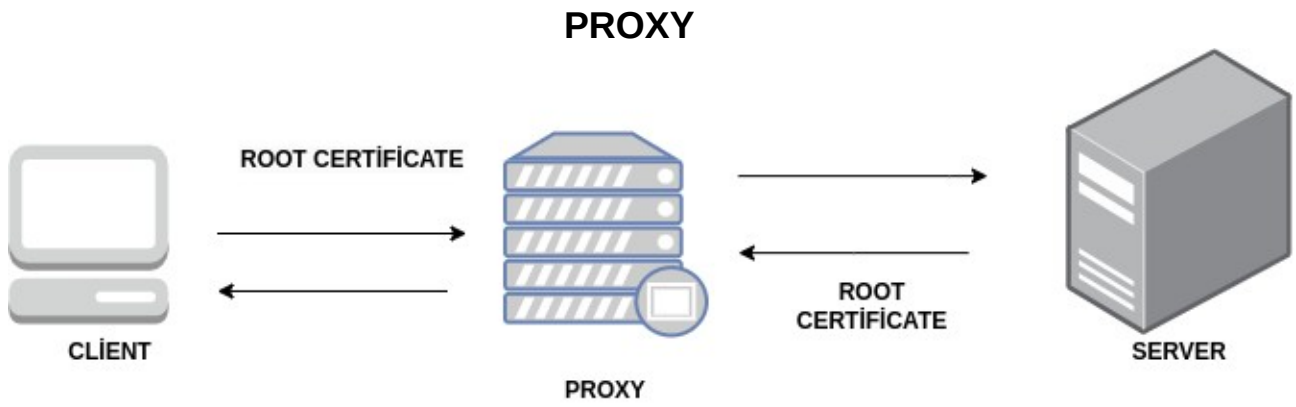
A | c

Burada ortak olan protokolleri seçer,yukarıdaki örnekte ise server ve client z,a protokollerini seçer.

```
vethd6b40dc: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::dc8d:faff:fee2:6058  prefixlen 64  scopeid 0x20<link>
        ether de:8d:fa:e2:60:58  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 138  bytes 21638 (21.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vlo1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 0c:54:15:5a:3a:02  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

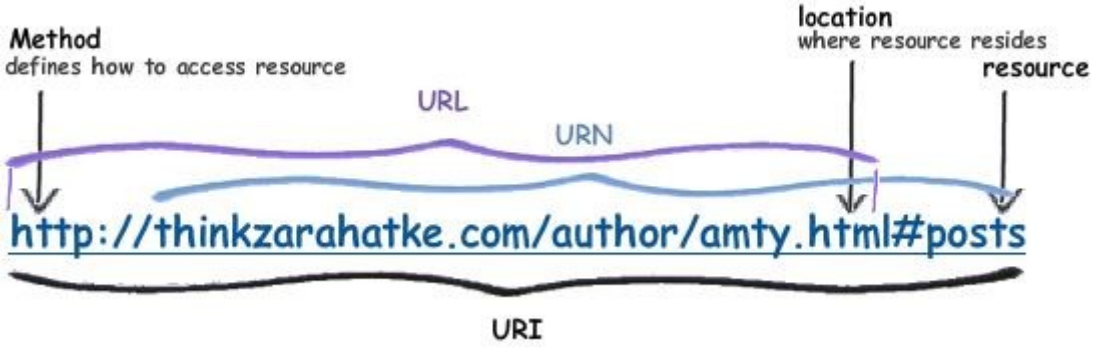
İnterface:internete giriş yapan her bir cihazın ,bir yada birden fazla arayüzü vardır(sanal makineler vb) ,her bir arayüz'ünde kendine ait ip adresi bulunur.



"Vekil sunucu" ya da "ara sunucu" olarak da bilinen Proxy, bağlanmak istediğiniz siteye başka bir kanal kullanarak geçmenize yarayan bir araçtır.

Kullanıcı olarak site adresinizi doğrudan İnternet tarayıcısına yazmak yerine, ücretsiz veya ücretli vekil sunucu hizmeti veren siteye yazabilirsiniz. Sunucu o sayfaya girer ve sizinle sayfanın içeriğini paylaşır.

URL & URI



https://user:pass@forum.omercitak.com:403/whoami/?search=1234&id=2#benkimim

#benkimim : anchor

?search=1234&id=2: query

/whoami/ :path

403:port

.com:tld

omercitak:domain

forum:subdomain

https://:şema

https:protokol

hackthebox

http-smugling:araştır

vga adaptörü getir

--HTTP REQUESTLERİ--

--raw request--

Güvenlik tarafında bir requesti ve responseları raw şekilde incelemek gerekiyor.Aşağıdaki bir requesti inceleyelim.

GET /gamma HTTP/1.1 **request header**

request body

Host: www.id-stat.com.tr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.id-stat.com.tr/gamma
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
request body
.
.
request footer (html vs burada)

--http status codes--

1.x.x	**info responselar**
2.x.x	**success responselar**
3.x.x	**direction(yönlendirme)**
4.x.x	**client hataları**
5.x.x	**servis hataları**