Deney 1

Gurbet Güngören

Veri sıkıştırma => Bir bilginin orjinal halinden daha az yer kaplayacak şekilde kodlanması olarak tanımlanabilir. Kayıplı/kayıpsız diye 2'ye ayrılır.

Kayıplı sıkıştırma => jpeg, mpeg-2, mpeg-4, mpeg-1 Vcd, H.265, H.264 Blu-ray, HD DVD, MP3, Vorbis, jpeg 2000,

Kayıpsız sıkıştırma => Lempel-Ziv (LZ), LZ Renau LZR (7ZIP), DEFLATE (PKZIP, GZIP, PNG), LZW GIF için, Aritmetik kodlama WMA9 Lossless, FLAC, ALAC Apple, DVD-Audio, Dolby TrueHD, Jpeg2000

Sıkıştırılmış veriler açıldığında, orjinal hale dönüldüğünde bu tür yöntemlere kayıpsız denir.

Metin dosyaları sıkıştırılırken 2 konuya dikkat edilmelidir.
1: Sıkıştırılacak veri, bir prog. dilinin kaynak koduna ait ise içindeki boşluklar zaten derleyici tarafından ihmal edileceği için, bu kısımlar sıkıştırmada kullanılabilir.
2: Bir kelime işlem programının çıktısı metin belgesi olarak kaydedilmek istenirse, font bilgisi gibi bilgiler ihmal edilebilir.

Sıkıştırıcı kodlayıcı: Giriş olarak tekrarın çok olduğu veri alınıp düşük tekrarlı dosya oluşturan kodlar.

Adaptif olmayan sıkıştırıcı: Bazı sıkıştırma algoritmaları hem veriyi inceleyip çalışmasını ona göre değiştiren yöntemlere adaptif sıkıştırıcı yöntemler denir. Huffman kodlama bu tip bir yöntemdir.

Bazı sıkıştırma algoritmaları 2 fazlıdır. İlk fazda sıkıştırılacak veri hakkında istatiksel bilgi toplanır, diğer fazında bu verilere elde edilen parametre ve kodlara bağlı olarak sıkıştırma olur. Bu yöntemlere yarı Adaptif yöntemler denir.

Simetrik sıkıştırma: Sıkıştırma ve sıkışmış verinin açılması aynı temel algoritmayı zıt yönlerde çalıştıran yöntemlerdir.
Sıkıştırma performansı için değişik büyüklükler kullanılır.

① En sık kullanılan sıkıştırma oranıdır. (compression ratio)

$$C.R = \frac{\text{Size of output file}}{\text{Size of input file}}$$

1'den büyük değerler sıkıştırılan dosya büyüklüğünün orjinal veriden daha fazla olacağından negatif sıkıştırma denir.

Sıkıştırma oranı ~~bpb~~ bpb (bit per bit) birimle ifade edilebilir
Resim için; bpp (bits per pixel)
Metin dosyaları için: bpc (bits per character)

Bitrate: bpb ve bpc için genel bir terimdir. (Temel hedef şiriken herhangi bir veriyi düşük bitrate ile ifade etmektir.

② Sıkıştırma oranının tersi ise sıkıştırma faktörü (compression factor)

$$C.F = \frac{\text{output}}{\text{input}}$$

Bu durumda 1'den büyük değerler sıkıştırmayı, küçük değerler genişlemeyi ifade edecektir.

(3) 100x (compression ratio) da anlamlı bir ölçüm performans göstergesidir. 60 değeri çıkış dosyasının orjinal dosyanın %40'ı kadar yer kapladığı anlamındadır. Ya da sıkıştırma ile %60'lık tasarruf edilmiştir.

(4) Resim sıkıştırmada bpp sıklıkla kullanılmaktadır. Bu bir pikseli sıkıştırmak için ortalama gerekli olan bit miktarını vermektedir.

Olasılık modeli; İstatiksel veri s. önemlidir. Bazı sıkıştırma algoritması 2 kısımdan oluşmaktadır probability model ve sıkıştırmanın kendisini ifade etmektedir.

Entropi; —

Deney 6 API Kullanımı

API, farklı programların birbiri ile iletişimini sağlayan protokollerdir.

Rest: Temsili durum transferi anlamına gelmektedir. API'lerin belli standartlara oturması için geliştirilmiş bir terimdir. Rest apilerin belirli özellikleri sağlaması gerekir. Bu özellikler Stateless, Uniform interface cacheable, Client-Server, Layered system, code on Demand olup
↳ Restful API denir tümünü sağlayan

Rest'de genelde json formatı kullanılarak bilgi alışverişi yapılır.

JSON ⇒ Özel olarak yapılandırılmış string ifadelerdir, objeler {}, diziler[] ifade edilir.

Genel olarak RestApi'ler güvenliği sağlamak için kullanıcı doğrulaması (authentication) gerektirir. Bu işlem API key veya tokenler ile gerçekleştirilir.

Api test araçları ve Postman

Api araçları sayesinde sorguların API dokümantasyonunda yer alan bilgilere göre düzgün bir şekilde gerçekleştirilip gerçekleştirilmediği test edilir. POSTMAN bu amaçla kullanılan bir Api aracıdır.

Postman ile header ve parametre bilgileri ile sorgular gerçekleştirilir.
Sunucudan dönen ifade RAW veya Pretty sekmesi altında görüntülenebilir.
↳ haberleşmede

Sık kullanılan Api Request Metotları → Sınavda boşluk doldurmada vardı.

GET: Genellikle sunucudan veri almak için kullanılan http metodudur. Sorgu ile gönderilmesi gereken parametreler URL içinde gönderilebilir.

POST: Parametreler hem URL ile hem de body bilgisinde gönderilebilir. Body bilgisinde gönderilen " gizlilik açısından daha etkili olmaktadır.

PUT: Genellikle veri güncellemek için kullanılan protokoldür.

DELETE: Genellikle " silmek için kullanılan protokoldür.

HTTP durum kodları

API'ler http protokolü üzerinden çalıştıklarından dolayı gönderdikleri hata kodları da http durum kodları ile aynı olmaktadır.

Postmann → 4xx hata kodu meydana geliyorsa, bu sorguda (parametre, uri, vs) hata olduğu anlamına gelmektedir.

http durum kodu sınıfları ~2022 vize sorusu

1xx: Gönderilen isteğin sunucuya başarılı bir şekilde ulaştığını ve işlemin başladığını bildiren kodlar (bilgi içeren mesajlar) içerir.

2xx: " " " " " " " " başarılı bir şekilde sonlandığını içeren dir içerir. (başarılı işlem mesajları)

3xx: Sunucunun başka bir adrese taşındığını durumlarda verilir (yönlendirme mesajları)

4xx: Gönderilen sorguda eksik veya yanlış ifadelerin olması durumunda sunucudan dönen dir. (istemci hatası mesajları). Bu başlıkta gelen hata kodları genellikle sorgunun yanlış veya eksik olmasından kaynaklı

5xx: Sunucu tarafından bir hata olduğunu ifade eden durum mesajlarıdır. (Sunucu hatası mesajları)

Sık karşılaşılan http durum kodları

200: İstemci ve sunucu arasındaki iletişimin başarılı olduğunu gösterir.
201: Gönderilen sorgu sonucunda sunucu tarafında bir verinin oluşturulduğu anlamına gelir.
400: İstek URI'sinin söz diziminde bir yanlışlık olduğunu ifade eder.
401: Sunucu-İstemci bağlantısı için kimlik doğrulaması gerekliliğini ifade eder.
403: Kimlik doğrulaması başarılı olup, kimliği doğrulanan kişinin ilgili URI'ye erişim hakkının olmamasını ifade eder.
404: URI adresinin sunucu tarafından bulunamadığını ifade eder.
405: Gönderilen request metodunun sunucu tarafından desteklenmediğini ifade eder.

2022 Finalde soruldu

Endpoint: Bir API ile bir istemci arasındaki bağlantının bir ucudur.
URI: İnternet üzerinde bir kaynağın tam yerine işaret eden (resim veya belge) standart formata uygun bir karakter dizisidir.
Bir kaynağı açık bir biçimde tanımlayan standart formata sahip bir karakter dizgisidir.

İstemci: Bir ağ üzerinde, sunucu bilgisayarlardan hizmet alan kullanıcı bilgisayarlarıdır.

Sunucu: Bilgisayar ağlarında diğer ağ bileşenlerinin erişebileceği, kullanımına veya paylaşımına açık kaynakları barındıran pc birimi.

JSON => Veri depolamak veya veri transferi gibi işlemler için kullanılmaktadır. (.json)
XML => " " için tasarlanmış bir biçimlendirme dilidir. (.xml)

* JSON, XML gibi geliştirilebilir bir yapı değildir.
* " , XML'e göre daha hızlı ve daha küçüktür.
* " da dizi desteği vardır. XML'de böyle kavram yok.
* JSON, XML'e göre daha kısa yazılır ve daha kolay okunabilmektedir.
* " çıkış noktası Javascript iken, XML markup dillerinden çıkmıştır.

Json formatında diziler ve nesneler (obje) nasıl ifade edilir?

obje (nesne) => { "no" : 1, "isim" : "Ahmet", }

diziler => "telefon" : [{ "tur" : "ev", "no" : "05__ " },]

Api test aracı nedir? En çok kullanılan?

Sorguların API dokümantasyonunda yer alan bilgilere göre düzgün bir şekilde gerçekleştirilip gerçekleştirilmediği test edilir.

ReadyApi, Accela, Katalon Stüdyosu, Postacı, DİNLENME garantili, Swagger.io, JMeter, Karate DSL, Havadan, Pyresttest, Apipee

Dağıtık programlama nedir? Dağıtık prog. niçin ihtiyaç duyulur?
Bir işin birden fazla pc tarafından yapılmasına denir.
* Bazı karmaşık programlar dağıtık pc'ler üzerinde çalışır.
Dağıtık prog. ölçeklenebilirliği arttırır.
Bazı yazılımlar vardır ki sadece belli donanımlara sahip bilgisayarlarda çalışırlar.
Güvenlik gerekçesi ile bazı servisler ayrı pc de olmak zorundadır.
Servislerin sadece kaynak olarak kullanıldığı durumlar.

Java da socket sınıfı ne işe yarar? Dağıtık prog. niçin socket sınıfı kullanılır?
İstemci oluşturmak için socket sınıfı kullanılır.

Java üzerindeki programların haberleşmesi için TCP ve UDP olmak üzere 2 farklı socket türü kullanır. Her ikisi de Client-Server ilişkisini kullanır haberleşmede.

Sunucu da 2010 nolu port açtıran ve istemcinin bağlanmasını bekleyen satırları yazınız. (2 satır) istemci bağlandığı zaman 'istemci bağlandı' yazdırın.
(Server tarafı)

```
ServerSocket soket = new ServerSocket(2010);
Sout("Bağlantı bekleniyor");

Socket baglanti = soket.accept();
Sout("Bağlantı gerçekleşti");
```

Client tarafı 2022-final sorusu

İstemciden 192.168.1.128 ip adresine sahip sunucunun 5040. portuna bağlanmak için gerekli nesneyi oluşturunuz.
Client tarafı

```
Socket baglanti = new Socket(192.168.1.128, 5040);
```

Soketten veriyi göndermek için kullanılan nesneyi oluşturun.

```
PrintWriter output = new PrintWriter(
    baglanti.getOutputStream(), true
);
output.println("gönderilecek mesaj");
```

Soketten veri almak için kullanılan nesneyi oluşturun.

```
BufferedReader in = new BufferedReader(
        new InputStreamReader(baglanti.getInputStream())
);
in.readLine();
```

Hash algoritması nedir? Sözlükte niçin kullanılmıştır?
Herhangi bir metnin şifrelenerek okunamaz veya önceden tahmin edilemez hale getirilmesi işlemidir.

Thread nedir? Ne işe yarar? Bu derecedeki kullanılma amacı nedir?

- Bir processin birden fazla işi aynı anda yapmasını sağlayan yapılara denir.
- Bir process bünyesinde bir ya da birden fazla thread barındırabilir. Çok çekirdekli işlemcilerde farklı çekirdeklerde eş zamanlı olarak çalıştırılabilirler.

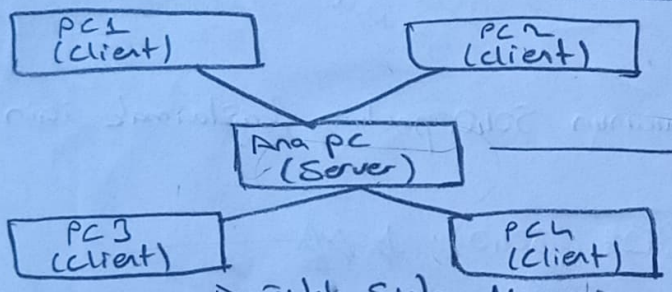
- Bir serverde birden fazla client bağlantısı dinlemek istediğimiz için, serverde oluşturduğumuz socket nesnelerini threadler yardımı ile oluşturduk dinledik.

Java programlama dilinde thread nasıl oluşturulur?

" da thread oluşturmak için sınıfı Thread sınıfından türetmek ve ardından run fonksiyonunu override etmek gerekir.
Thread sınıfından türetilen nesnenin start metodu çağrıldığında, run içerisine yazdığımız kodları tetikler.

MD5 nedir?

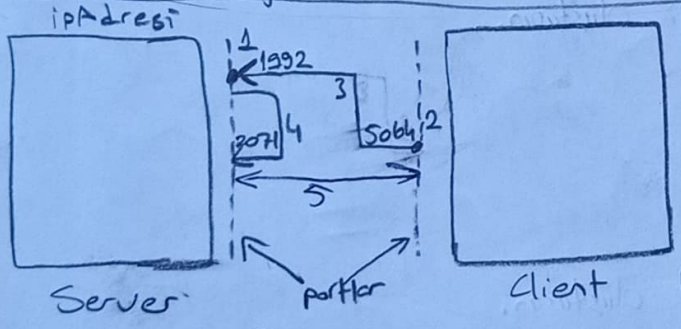
Tek yönlü bir hashing algoritmasıdır. Çıkışta 128 bit veri üretir.



Dağıtık Sistem Mimarisi

İşn 512
x 30x20x40x60

(1,25)→32



① Müsait bir port dinlenir (şekilde 1999 seçilmiş)
② Server pc'nin açılan portuna bağlantı denemesinde bulunur (ipadresi, 1992 parametreleri ile)
③ Porta ulaşınca bağlanma gerçekleşir.
④ ServerSocket nesnesi accept() fonksiyonu aracılığıyla boş bir port açarak gelen isteği bu port ile eşleştirir.
⑤ 2 pc açılan portlar aracılığıyla iletişim sağlar (2071 ve 5064)

2022 Vize Sorusu

Şekil verilmiş. Adımlarını açıklayın denmişti.

Yapay Sinir Ağları

Yapay sinir hücrelerinin birbirine bağlanmasıyla oluşan yapılardır.

Perceptron Öğrenme Algoritması

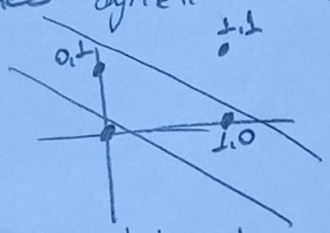
Denetimli bir öğrenme algoritmasıdır. P. Modelinde en önemli faktör eşik değeridir. Gözlenlenmiş verileri kullanarak yeni gelecek verilerin sonuçlarını tahmin etmede kullanılır.

Aktivasyon fonk. sayesinde doğrusal olarak ayrılmayan veriler, doğrusal olmayan şekilde ayrılabilirler. " " verileri dönüştürmeye farklı bir boyut kazandırmaya yarar.

Perceptron, tek katmanlı ileri beslemeli nöral ağıdır.

VE kapısı lineer ayrıştırılabilir. XOR kapısı lineer ayrıştırılamamaktadır. (tek 1 doğru yeterli değil)

x_1	x_2	XOR
0	0	0
0	1	1
1	0	1
1	1	0



en basit non-lineer problemdir.

XOR çok katmanlı algılayıcıların geliştirilmesi ile çözüme ulaştı

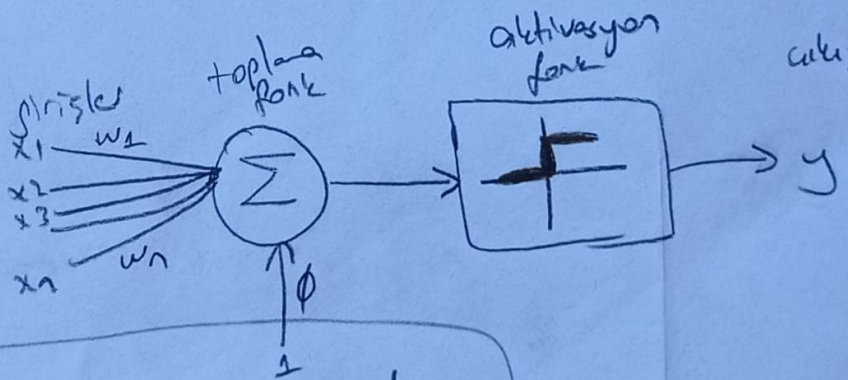
İleribeslemeli ağ → Herhangi bir nöronun çıkışı, sadece ve sadece bir sonraki katmanda bulunan nöronlar için giriş olarak kullanılır. bu çıkış önceki katmandaki veya aynı katmandaki nöronlara giriş olarak verilmez. (ÖR/ Adaline, Perceptron)

Geri beslemeli ağ → Herhangi bir nörondan alınan çıkış, aynı katmandaki veya bir önceki katmandaki nöronlara giriş olarak verilebilir. Eğitim süreleri daha uzundur.

ÖR Boltzman Machine
Recurrent Time Series

Yapay sinir ağı 3 katmanda oluşur. (giriş katmanı, gizli katman, çıkış katmanı)

Perceptron



girişler
ağırlık
toplama fonk.
aktivasyon fonk.
çıkış

Sınavda XOR kapısını sormuştu.
↳ 2022 final

1-Ödev

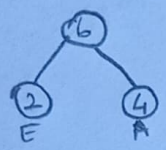
Gurbet Günpören

Karakter	Frekans
A	4
B	16
C	8
D	26
E	2
F	45
G	85
H	25

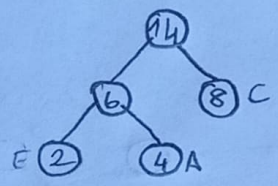
2	4	8	16	25	26	45	60
E	A	C	B	H	D	F	G

2022 Vize ve final de soruldu.

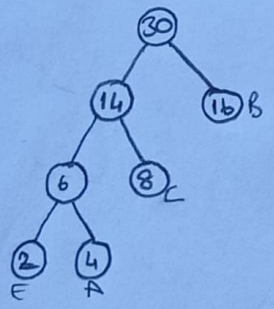
Adım 1: 2 ve 4 en küçük sayılardır. Bunları birleştiririz.



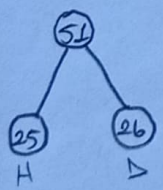
Adım 2: Ağacın kökü ve 8 en küçük ikili bunları birleştiririz.



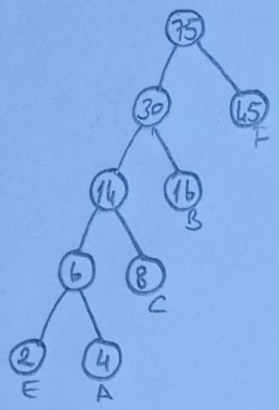
Adım 3: 16 ve ağacımızı birleştiririz.



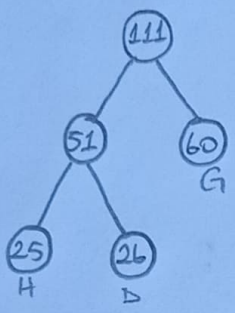
Adım 4: Ağacın kökünden daha düşük frekansa sahip iki tane karakterimiz var. Bunları alıp yeni bir ağaç yaparız.



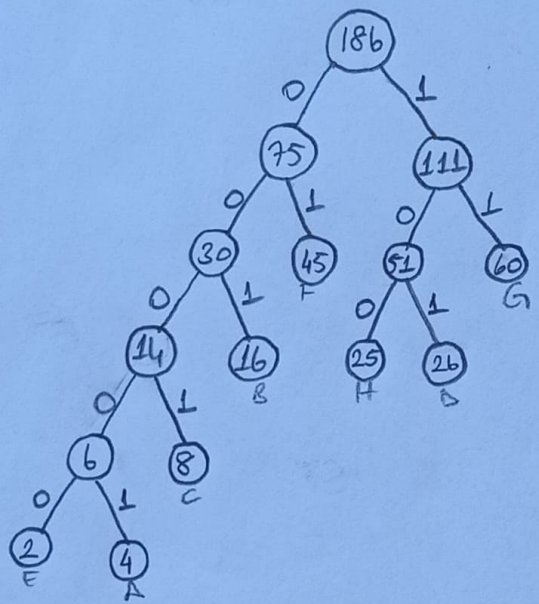
Adım 5: Birinci ağacımız ile 45 sayısını birleştiririz.



Adım 6: 60 ile ikinci ağacımızı birleştiririz.



Adım 7: Oluşan iki ağacımızı birleştiririz.



A=00001
E=00000
C=0001
B=001
H=100
D=101
F=01
G=11

Örnek: HECE $\Rightarrow 4 \times 8 = 32$ bitlik veri

10000000000100000 $\Rightarrow$ 17 bitlik veri

* 32 bitlik veriyi huffman kodlama ile 17 bite sıkıştırılmış oldu.

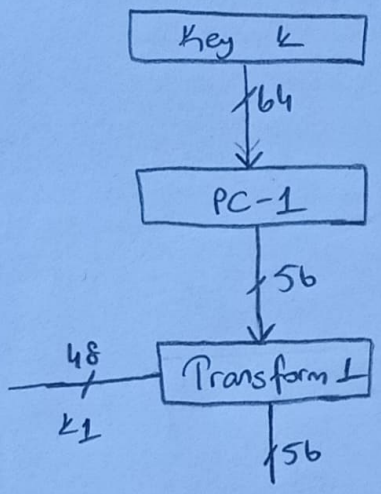
Gurbet Günpören

Ödev-2

PC-1 aşamasında yapılan işlemler;

Des algoritmasının başlangıçta 56 bite sahiptir. 16 adımdan oluşur. Her bir adımda farklı anahtarlar kullanılıyor. 64 biti 8 bitlik bloklara ayırıyoruz. Parity biti anahtar iletilirken hata olup olmadığını denetlemeye çalışır. Orjinal de anahtarımız 64 bittir ama 8 biti parity biti olduğu için 56 bite indirgiyoruz.

Daha sonra 56 biti 48 bite indirgiyoruz. Bunun için de PC-1 permütasyonu kullanıyoruz. Veri de belli parametredeki değerleri almayarak veri üzerinde bir permütasyon işlemi gerçekleşiyor.



Anahtar Planlama Algoritması

Transform-1 aşamasında yapılan işlemler;

56 bitlik anahtarı 2 paraya ayırıyoruz. 64 bitlik bir anahtarımız vardı. Bu anahtarın son 8 bitini kullanmayarak 56 bite indirdik. 2 paraya ayırdık. (28-28) Daha sonra çeşitli miktarlarda sağa kaydırma işlemine tabi tutulur. 1, 2, 9, 16. adımlarda bunlar. 1 bit devirsel olarak rotate edilir. Diğer tüm adımlarda 2 defa rotate edilir. Toplam 16 adımdan oluşuyordu. 12 adım da 2 bit 4 adımda 1 bit rotate edilir. Daha sonra PC-2 permütasyonundan veriyi geçirerek bir karıştırma işlemine tabi tutulur.

Penetrasyon Testi

Esra Gündoğan
deneyap

Bilgisayar ağının ya da sisteminin içeriden ya da dışardan gelebilecek saldırılara karşı ne kadar güvende olduğu konusunda fikir edinilmesini sağlar.

Dos testi => Şirketin bir saldırıda hizmetlerinin çöküp çökmeyeceği test edilir (dayanıklılığına bakılır)
Application => Kullanılan uygulamalar ve kodlarında açık taraması yapılır.
Dış ağın pt. => Yapılanmanın dış dünyadan gelebilecek herhangi bir tehdide karşı durumu tespit edilir.

Faydaları

Saldırılara karşı daha dirençli bir bilişim altyapısı
Kullanıcı bazlı olarak bilgi güvenliği farkındalığının artması
Sistemlerin durdurulma veya kaynak doldurmaların engellenmesi
Yasal olarak uyum sağlama
Marka değerinin korunmasını sağlar.
BT kaynaklı risklerinin azalması

whois, hedefin alan adını ve dns sunucularını verir.

2022 Final sorusu

Penetrasyon Testinin Adımları

Bilgi toplama => Sistem hakkında ön bilgi edinmek.
Tarama => Sistemi tarayarak bilgi edinmek.
Erişim sağlama => Sistemde bulunan açıklar kullanılarak sisteme izinsiz erişim sağlanması.
Erişim koruma => Elde edilen erişimlerin korunması.
İzleri yok etme => İlk 4 adımda yapılan işlemlerin bıraktığı izler temizlenir veya kirletilir.

Ağ güvenliği test ve denetim araçları

* Ağ dinleme araçları -> Wireshark, Pinğ ve Ping Sweeps
* Port tarayıcılar -> NMap, HTTrack
* Şifre kırma araçları -> Medusa
* Web güvenlik test -> Paros, Netsparker, Webinspect, Acunetix Web Vulnerability Scanner
* Genel amaçlı güvenlik açığı tarayıcılar -> Nessus, Metasploit, Qualys

2022 - Vize
↳ Wireshark, NMap — us verilmiş hangi araç grubuna girer diye sorulmuştu

Lineer Kriptanaliz -> Düz metin, şifreli metin ve döngü anahtarlarının bitleri kullanılarak oluşturulan lineer denklemlerinin doğru olmasını kullanılarak yapılan atak işlemidir.

Kriptoloji => Şifre bilimidir.

Kriptografi => Bir verinin içerdiği bilginin istenmeyen taraflarda anlaşılmayacak bir hale dönüştürülmesinde kullanılan yöntemlerin tümüdür.

Kriptanaliz => Şifre ya da anahtar kullanmadan deşifre etme yöntem ve prensipleri.

Simetrik şifreleme => Bilgileri şifrelemek ve deşifre etmek için yalnızca bir gizli anahtar içeren en basit şifreleme türüdür.

Asimetrik şifreleme => Şifre ve deşifre işlemleri için farklı anahtarlarının kullanıldığı bir şifreleme sistemidir. Tarafların her birinde birer çift anahtar bulunur.

Des Algoritması => Dünyada en çok kullanılan simetrik şifreleme algoritmalarından birisidir. Blok şifreleme kullanan DES, işlem sırasında 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler. Anahtar uzunluğunun kısa olması nedeniyle kırılmıştır. SSH gibi uygulamalarda kullanılır günümüzde.

Tarih ve İşyeri Amirinin İmzası	...../...../20...