**1.HAFTA:**

Ders genel işleyiş

**2.HAFTA:**

Proje Konuları

**3.HAFTA:**

Bilgi, öznitelik…

**4.HAFTA:**

YOKTUM

**5.HAFTA:**

\*\*ÖNEMLİ BİR KONU—

BÖLÜM-4 – NOTLAR:

KESİN SORU GELECEK

Wireshark (paketleri izliyor, dinliyor, görüyor.) –Ağ dinleme ve izleme aracı:

Wilmax – uzun mesajlar (kampüs ağları):

Güvenli işletim sistemleri:

AĞ GÜVENLİĞİ- BİLGİ GÜVENLİĞİNİN ALT DALI:

Ben mesaj gönderirsem oraya nasıl gidiyor?- aradaki işlemler neler? OSI katmanları.

Doküman currose ve rose kitabından alıntı (15-20)

Router nedir ?

Global ISP nedir?

SWITCH Nedir?

Access Point Nedir? > Modem

Switch

Router

Modem

İçerir.

Modülasyon (doğrultma) nedir?

Acces point türleri = ADSL, VDSL

Switch nedir? – bilgisayarların ortak noktası.

KAMPÜS NETWORK DETAYLI:

Hub cihazı nedir?

Switch nedir?

Kamps network hub ve switch içeriyor.

Hub port içeriyor- van limanı.

Hub internete bağlanır –

Bir bilgisayar diğerine mesaj

OSI KATMANLARI:

1. Application
2. Presentation
3. Session
4. Treansport
5. Network
6. Data link
7. Physical

MAC Adresleri her bilgisayar için benzersizdir.

Ağ katmanı burası:

Network header kendi için de ikiye ayrılıyor- source and destination ip tutulacak. Nereye gönderdiğini nereden bilecek?

Mac header kendi içinde ikiye ayırılıyor source and destination mac adresi .

Fiziksel katmanda veriler 010101 oluyor?

HUB CİHAZI- APTAL MAKİNE – PASİF ELEMAN- AKILSIZ DAĞITICI(1.katmanda çalışıyor)

Görevi: Kendisine gelen elektriksel sinyalleri güçlendirir. Hub bütün portalara veriyi gönderir.

192.168.1.1.:80 80 port numarası- İp Numarası

İp adresi ev adresi gibi (tokat/tekke köyü) mac adresi kişisel benlik gibi(Ahmet oğlu Necdet)

MAC-SPOOFİNG- MAC ALDATMACISI- mac adresimi değiştirip, mesajı alırım

IP SPOOFİNG – IP ALDATMACISI – ip adresimi değiştirip, mesajı alırım.

IP Sniffing- Mac sniffing – Wireshark ile tüm paketleri alırım, işime yarayanı alırım.

Presentation katmanı şifreleme çözülüyor. Mesaj elimde ama okuyamıyorum albayım.

HUB YERİNE SWİTCH OLURSA NE OLUR?

Switch kendi içinde mac adres listesi tutuyor. 8 portlu bir mac adresi bilgisi.

Switch hedef mac adresinin portunu biliyor ve sadece oraya gönderiyor

Hub ise tüm portlara gönderiyor.

HUB VS SWİTCH- GENEL KONUŞULAN KONU

Omurga denilince akla router gelmelidir. – Layer3’te router çalışır.

Router iki nokta arasındaki en kısa yolu bulmaya çalışıyor. Yazılımı ise routing protocol- PUP,IGRP,OSPF,EIGRP

Yönledirme OSI katmanının 3.katmanında yapılıyor.

WİRESHARK ÖZELLİKLERİ:

Ağ trafiği

Veri madenciliği

Port tarama

Vs

Wireshark bileşenleri nedir?

**6.HAFTA:**

ŞİFRELEME BİLİMİ VE TEKNİKLERİ:

Şifremele güvenliğin alt dalıdır.

Applied mathmetic – uygulamalı matematik

KRİPTOLOJİ BUGÜNKÜ DERSTE ANA BAŞLIK OLARAK GEÇİYOR:

Şifreleme algoritmaları bilgi güvenliği kapsamında (wifi,kablosuz,dosyalama,blokzincir) kullanılmaktadır.

KRİPTOLOJİ BİLİMİ ALTINDAKİ YAPILAR:

Kriptografi:Bilgiyi şifreli hale dönüştürme işlemidir.

Kriptoanaliz: Şifreyi çözmeye çalışmak.

Şifreleme = Encyripthon

Şifre çözme = Descriptin

PAROLA! = ŞİFRE

ŞİFRELEME ALGORİTMALARI İÇİN ALGORİTMANIN GENEL ÖZELLİKLERİ GEÇERLİ

Anahtar: Şifrenin nasıl elde edildiğine dair kod parçasıdır.

SEZAR ŞİFRELEME:

Önemli Mesaj:

11.11.2011;

Şifreleme sunum - Presentation (☺) katmanında yapılır.  
  
PİGPEN- MASON ŞİFREMELESİ:

PROMİS

ENİGMA:

STEGANOGRAFİ:

Gizlenmiş yazı anlamına gelmektedir.  
Resim içine bilgi gizleme

Ses içine bilgi gizleme

Video içine bilgi gizleme

Network alanında kullanılıyor.

HASH:

Log analizi için kullanılıyor.

Hash için geri dönüşüm yoktur.

Kimyasal reaksiyon tarzında bir şey

MD5: (Message Digest Algorithnmas)

Oktay

F5503rıwngpınfwnfvq

SH1: (Secure hash algortihm):

SHA-1

SHA-2 algoritmları

SHA- 256 algoritması:

DES: (Veri şifreleme):

Data encrypthon algoritması baz alır

RSA Açık anahtar algoritması

TEMEL MATEMATİK KULLANILIYOR:

Şifrele = c = me mod n

Şifre aç : m=c , d=mod n

BitLocker:

Windows 7 işletim sisteminde kullanılıyor:

WEP ŞifrelemeÇ

Wired Equivalent Priacy – Daha çok kablosuz ağlarda kullanılıyor:

WPA Şifreleme:

Kablosuzun babası:

İki mode wpa-psk

;