**UTİ513 Bilgi, Güvenlik ve Mahremiyet**

**FİNAL SINAVI**

**15 Ocak 2014**

**İki A4 yardım kağıdı. İstediğiniz 4 soruyu yanıtlayınız. Süre 120 dakika.**

**1.**

1. Theft of intellectual property
2. Theft of other (proprietary) info including customer records, financial records, etc.
3. Denial of service attacks
4. Virus, worms or other malicious code
5. Fraud (credit card fraud, etc.)
6. Spam e-mail. Computer as communications tool.
7. Phishing
8. Unauthorized access to/use of information, systems or networks
9. Sabotage: deliberate disruption, deletion, or destruction of information, systems, or networks
10. Web site defacement

Yukarda listelenen siber suçların her biri için

**a)** Bilgisayarın hedef mi, depolama ortamı mı yoksa iletişim aracı mı olarak kullanıldığını,

**b)** Bilgisayarların hedef olduğu siber suçlar için saldırının hangi güvenlik servisine ya da servislerine karşı (gizlilik, bütünlük, mahremiyet, erişilebilirlik (*availability)*) yapıldığını yazınız.

**2.**

****

Yukarda verilen erişim matrisi için

1. Erişim kontrol listesini çiziniz. **(9 p)**
2. Yetenek Listesini (ing. *Capability List*) çiziniz. **(9 p)**
3. Bu iki yaklaşımın avantaj ve dezavantajlarını, karşılaştırmalı olarak yazınız. **(7 p)**

**3. a)** Üç temel saldırgan sınıfını (ing. *3 classes of* *intruders)* yazıp, her birini kısaca açıklayınız.

**b)** Bir Sızma Tespit Sisteminde (ing. Intrusion Detection System) yer alan üç temel bileşeni ve görevlerini yazınız.

**c)** Host-tabanlı Sızma Tespit Sistemleri ile Ağ-tabanlı Sızma Tespit Sistemleri arasındaki farkları yazınız.

**d)** Bir Sızma Tespit Sisteminin sağladığı üç temel faydayı yazınız.

**4.** SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail

between hosts over TCP. A TCP connection is set up between a user agent and a

server program. The server listens on TCP port 25 for incoming connection requests.

The user end of the connection is on a TCP port number above 1023. Suppose you

wish to build a packet filter rule set allowing inbound and outbound SMTP traffic.

You generate the following rule set:

****

**a**. Describe the effect of each rule.

**b.** Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are as shown:

****

Indicate which packets are permitted or denied and which rule is used in each case.

**5. a)** Bell La Padula **(BLP)** Güvenlik Modelindekullanılan üç kuralı tanımlayınız.

**b)** Aşağıdaki şekilde üst sağ köşedeki rol BLP modelindeki kuralları ihlal etmeden bir kullanıcıya

atanabilir mi? Açıklayınız.

****

**6.** Avrupa Birliği Veri Koruma Yönergesi (European Union Data Protection Directive)

a) Bu yönergenin amacı nedir? (**4 p**)

b) Bu yönergede yer alan *Notice, Consent, Consistency, Access, Security, Onward Transfer* ve

*Enforcement* ilkelerini kısaca açıklayınız. (**21 p**)