**UBI528 Ağ Güvenliği Teknikleri**

**FİNAL SINAVI**

**7 Haziran 2017**

**Dilediğiniz 8 soruyu yanıtlayınız. Her soru 12 puandır. Sonuca 4 puan eklenip sonuç 100’e tamamlanır.**

**İki A4 yardım kağıdı. Yanıtlamadığınız soruları soru kağıdı üzerinde açıkça işaretleyiniz. Süre 2 saat**

**1.** Aşağıdaki ifadeleri “doğru” yada “yanlış” olarak etiketleyiniz. Her doğru yanıt +1,5, her yanlış yanıt -1 puan.

**i)** Bir Müşteri-Sunucu ortamında CBC modunda çalışan bir blok şifreleme tekniği kullanıyor. Bu durumda taraflar kullandıkları IV değerlerini birbirlerine şifrelenmemiş olarak gönderir.

**ii)** Host A’dan Host B’ye IPSec kullanan bir paket akışı (*stream of packets*) olsun. Bu akıştaki her paket için yeni bir SA (*Security Association*) kurulur.

**iii)** Skype’da bazı mesaj başlıkları hariç tüm paket içeriği şifrelenmektedir.

**iv)** Klasik paket filtreleme cihazlarında her arayüzün (*interface*) kendi erişim denetim listeleri olabilir.

**v)** Yapısal hiçbir açığı olmayan ve 80 bit uzunluğunda çıktı üreten bir öz (*hash*) fonksiyonu günümüz standartlarına göre güvenlidir.

**vi)** Skype kullanıcı doğrulama protokolünde taraflar daha önce Skype sunucusundan edindikleri kendilerine ait açık anahtar sertifikalarını karşılıklı olarak birbirlerine gönderirler.

**vii)** SSL’de şifreleme ve bütünlük (MAC) için aynı anahtar kullanılır.

**viii)** Bir mesajın özünü (*hash*’ini) deşifre edip (*decrypt*) orijinal mesajı elde etmek mümkündür.

**2. a)** Virüslerle worm’lar arasındaki temel fark nedir? Polymorhic virüs nedir? Açıklayınız.

**b)** Tekrar oynatma (*replay*) saldırılarına karşı savunma için hangi mekanizmalar kullanılır? Açıklayınız.

**c)** Alice dünyaca ünlü bir aktivist ve elinde tüm dünya ile paylaşmak istediği bir mesajı var. Binlerce insan Alice’in mesajını almak istiyor, fakat her biri mesajın bütünlüğünden (*integrity*) emin olmak istiyor. Bu senaryoda MAC-tabanlı mı yoksa sayısal imza tabanlı mı bir mesaj bütünlüğü yöntemi daha uygundur? Açıklayınız.

**3.** SPF ve DKIM çöp e-postaya (*spam mail*) karşı geliştirilmiş iki savunmadır.

SPF’de e-postayı alan sunucu makina (*receiving email* *server*) e-postadaki “From:” satırındaki alan ismi (*domain name*) için bir DNS sorgusu gerçekleştirir ve o domain’den e-posta göndermeye yetkili (*authorized*) makinaların IP adres listesini DNS yanıtı içinde elde eder. Kontrol ettiği e-postanın geldiği IP bu listede yok ise mesajı spam olduğu gerekçesi ile reddeder.

DKIM’de ise gönderici e-posta sunucusu mesajı özel (*private*) anahtarı ile sayısal olarak imzalar. Bu e-postayı alan sunucu makina (*receiving email server*) e-postadaki “From:” satırındaki alan ismi (*domain name*) için bir DNS sorgusu gerçekleştirir ve o domain’e ait açık anahtarı (*public key*) DNS yanıtı içinde elde eder. Ardından bu açık anahtar ile elindeki e-postanın üzerindeki imzanın gerçekten o domain’e ait olup olmadığını doğrular. Doğrulama sağlanırsa e-postayı kabul aksi takdirde reddeder.

SPF üzerinde çalışan ancak DKIM’e karşı çalışmayacak yaygın bir saldırı tekniği vardır. Bu saldırı nedir? Açıklayınız.

**4. a)** Uygulama geçidi (ing. application gateway; aynı zamanda proxy gateway olarak da bilinir) nedir? Ne amaçla kullanılır?

**b)** Uygulama geçitlerinin avantajları ve dezavantajları nelerdir?

**5**. Alice ve Bob ortak parametreler ***g*** ve ***n***’i biliyor olsunlar. Alice ve Bob aşağıdaki protokolü kullanarak anahtar değişimi yapmak istiyorlar.

1. Alice sadece kendisinin bileceği bir *x* değeri seçer ve $K\_{B}^{+}$($g^{x}$mod n) değerini Bob’a gönderir.
2. Bob sadece kendisinin bileceği bir *y* değeri seçer ve $g^{y}$mod n, H($g^{xy}$mod n) değerini Alice’e gönderir.
3. ?
4. Protokolün üçüncü adımında Alice ortak anahtarı $K\_{AB} $‘yi nasıl hesaplarlar?
5. Mesaj trafiğini dinleyebilen üçüncü bir kişi, Carol, Alice’i kendisinin Bob olduğuna ikna edebilir mi? Açıklayınız.
6. Carol tüm mesajları kopyalamış ve daha sonraki bir zamanda da Bob’un özel (private) anahtarını ($K\_{B}^{-}$) ele geçirmiş olsun. Ortak anahtar $K\_{AB}$’yi elde edebilir mi? Açıklayınız.

**6**. **a)** “*Cross Site Scripting (XSS)*” saldırısı nedir? Nasıl çalışır? Açıklayınız.

**b)** “*Same origin policy*” nedir? XSS saldırısı ile bağlantısı nedir? Açıklayınız.

**7.** Bir şirket ağ geçidi (*gateway*) üzerinde konuşlandırılmış durumsuz (*stateless*) bir paket filtreleme güvenlik duvarı (*firewall*) olsun. Şirket ağına giren çıkan tüm trafiğin bu güvenlik duvarından geçtiğini varsayalım. Güvenlik duvarı kural formatımız aşağıdaki gibidir:

**Action SourceIP SourcePort DestIP DestPort**

**a)** Şirketin iç ağında yer alan ve belli bir IP’ye sahip (örneğin 192.46.20.04) bir Web sunucusuna dışardan HTTP bağlantısını engellerken aynı sunucuya dışardan HTTPS erişimine izin vermek bu paket filtereleme güvenlik duvarı ile sağlanabilir mi? Sağlanabilir ise ilgili güvenlik duvarı kurallarını yukardaki formata uygun olarak yazınız. Sağlanamaz ise açıklayınız.

**b)** Bir paket filtreleme güvenlik duvarı ile içinde “V1AGRA” kelimesi geçen tüm e-posta mesajlarını bloke edilebilir mi? Yanıtınız Evet ise ilgili güvenlik duvarı kuralını yukardaki formata uygun olarak yazınız. Hayır ise neden?

**8.** Elimizdebulunan bir Sızma Tespit Sisteminin (IDS) yanlış pozitif oranı %8, yanlış negatif oranı ise %10’dur. Bu IDS üzerinden geçen paketlerin %98’inin normal %2’sinin ise saldırı paketleri olduğu bilinmektedir.

**a)** Bu IDS üzerinden on bin saldırı paketi geçtiğinde bunlardan kaçını normal olarak işaretleyecektir?

**b)** Bu IDS üzerinden 1 milyon normal paket geçtiğinde bunlardan kaçını saldırı paketi olarak işaretleyecektir?

**c)** Bu IDS tarafından saldırı paketi olarak işaretlenen bir paketin gerçekte normal olma olasılığı nedir?

**9.** **a)** Ağ güvenliği bağlamında Bal çanağı (*Honey Pot*) nedir? Nasıl kullanılır?

**b)** Bir ağda bal çanağını iç ağa (*Internal Network*) yerleştirmenin avantajları ve dezavantajları nelerdir?

**10. a) iptables** nedir? **İptables**’da kullanılan NAT tablosu ne işe yarar?

**b)** Bilgisayarımızayeni bir bağlantı açmayı hedefleyen tüm içe doğru gelen (*incoming*) SYN paketlerini reddetmek için gerekli **iptables** komutunu yazınız.