**UBI528 Bilgisayar Ağ Güvenliği**

**ARASINAVI**

**28 Mart 2024**

**Bir A4 yardım kağıdı. Her soru 20 puan. Dilediğiniz altı soruyu yanıtlayınız. Süre 90 dakika.**

1. Aşağıdaki ifadeleri doğru ya da yanlış olarak işaretleyiniz.

(Her doğru yanıt +2, her yanlış yanıt -1 puan.)

1. SYN cookies SYN taşkını saldırısına karşı bir savunma aracıdır.
2. *Traceroot* hedefe giden yol üzerindeki yönlendiricilerden (*routers*) aldığı “*TTL Expired*” ICMP paketlerini hedefe giden yolu tespit etmek için kullanır.
3. AH (Authentication Header) bir SSL alt protokolüdür.
4. MD5 iyi bilinen bir öz (hash) algoritmasıdır.
5. Üçlü DES (3DES) anahtar uzayı tarama saldırısına karşı tekli DES’den en fazla üç kat daha güçlüdür.
6. Saldırgan hedef ağdaki canlı makinaları (*hosts*) belirlemek için port taraması ve canlı servisleri belirlemek için *ping* taraması kullanır.
7. Saldırı öncesi keşif (*reconnaissance*) çalışması için temel iki kaynak **Whois** ve **DNS** veritabanlarıdır.
8. Bir makine beklemediği bir TCP paketi aldığında RST biti set edilmiş bir TCP paketi ile yanıt verir.
9. Bir makine beklemediği bir UDP paketi aldığında ICMP “*port unreachable*” paketi

ile yanıt verir.

1. Aşağıdaki nmap komutu google.com alanındaki tüm TCP default portlarını tarar.

nmap –v google.com

**2.** Alice Bob'a **güvenli elektronik posta** göndermek için aşağıdaki protokolü kullanıyor.

Alice → Bob: $K\_{A}^{-}$(H(m)) || m

m mesaj, $K\_{A}^{-}$ Alice'in gizli anahtarı, || ekleme işareti, H( ) halka açık (*public*) hash fonksiyonu

1. Bu e-posta protokolünde gizlilik (*confidentiality*), doğrulama (*authentication*) ve bütünlük (*integrity*) servislerinden hangileri sağlanmaktadır? Neden?
2. Yukardaki protokolde gizlilik sağlanmıyorsa, sağlamak için protokole gereken eklemeyi yapınız.

**3.** Aşağıdaki ağ konfigürasyonunda saldırganın (*attacker*) kurbana (*victim*) giden gelen paketleri nasıl dinleyebileceğini açıklayınız. Bu dinlemeyi engellemek için neler yapılabilir?

 

**4. a)** Dağıtık Hizmet Engelleme Yansıtma Saldırısı (*DDoS Reflection Attack*) nedir? Kısaca Açıklayınız.

**b**) Normal bir IP datagramının bir IPSec datagram’ına nasıl dönüştürüldüğünü anlatınız.

**5**. Aşağıdaki oyuncak-WEP protokolünde anahtar 4 bit, IV ise 2 bit uzunluktadır. Anahtar bitlerini (ing. *keystream*) üretirken IV 4-bit anahtarın sonuna eklenmektedir. Ortak gizli anahtar 1010 olsun. Anahtar + IV’nin dört farklı birleşimi için üretilen anahtar bitleri aşağıda verilmiştir.

101000: 0010101101010101001011010100100 …

101001: 1010011011001010110100100101101 …

101010: 0001101000111100010100101001111 …

101011: 1111101010000000101010100010111 …

WEB ile şifrelenecek mesajlar 8-bit, ICV (*Integrity Check Value*) 4-bit uzunlukta olsun. Ayrıca ICV, mesajın ilk 4 bitinin ikinci 4 biti ile XOR’lanması ile hesaplanıyor olsun. Oyuncak WEP paketleri üç alandan oluşsun: Önce 2-bit IV alanı, ardından 8-bit mesaj alanı ve en sonda ise 4-bit ICV alanı. Bu alanlardan bazıları WEP protokolündeki gibi şifrelidir.

**a)** IV = 11 ve mesaj *m* = 01101001 olsun. Gerekli işlemleri yaparak Oyuncak-WEP paketini oluşturunuz.

**b)**  Alıcı tarafa 11010010011100 şeklinde bir WEP paketi gelsin. Yapılan işlemleri ve bulunan açık mesajı gösteriniz. Bu paket bütünlük (ing. *integrity*) kontrolünü geçer mi?

**6.**



**a.** Şekilde yönlendiriciler R1 ve R2 arasında kurulmuş bir Güvenlik İşbirliği (ing. Security Association (SA)) görülmektedir. R2’de bu SA için hangi bilgiler tutulmaktadır. Bu bilgi başlıklarını ve mümkün ise ilgili başlıklar için somut değerleri (örn. hedef IP vb.) yazınız.

**b.** Aşağıdaki ifadelerin doğruluğunu yada yanlışlığını yukardaki şekli dikkate alarak kısa açıklamalarla belirtiniz.

**i)** 172.16.1/24 adresindeki host Amazon.com sunucusuna bir datagram gönderdiğinde yönlendirici R1 datagramı IPsec kullanarak şifreleyecektir.

**ii)** 172.16.1/24 adresindeki host 172.16.2/24 adresine bir datagram gönderdiğinde yönlendirici R1 bu datagramın kaynak ve hedef adreslerini değiştirecektir.

**7.** SSL’in ilk versiyonları “*cipher suite rollback*” adı verilen bir saldırıya açıktı. Müşterinin SSL el-sıkışmasını başlatmak için gönderdiği “Hello” mesajı doğrulanmamıştır, ki bu mesaj aracılığıyla müşteri desteklediği kriptografik algoritmaları karşı tarafa (sunucuya) ilan eder, bir saldırgan (mesela Trudy) bu mesajı değiştirebilir ve sunucuyu müşterinin sadece görece zayıf algoritmaları desteklediğini düşündürebilir. Bizim derste işlediğimiz SSL versiyonunda bu saldırıya karşı önlem alınmıştır. Bu önlem nedir ve bu saldırıya karşı nasıl koruma sağlar? Açıklayınız.