Wireshark Egzersiz – 1

Son Teslim Tarihi: 13.04.2020 23:00 (Moodle)

Web site adresi: http://www.altoromutual.com/login.jsp

Yukarıdaki web site adresini istediğiniz bir internet tarayıcısının adres kısmına giriniz ve Wireshark programı üzerinden aşağıda istenen maddelere göre trafik akışını dinleyiniz.

1. Tarayıcınız üzerinden yukarıdaki web adresine erişmeye çalıştığınızda web site sunucusu ile bilgisayarınız arasında TCP-handshake gerçekleşmesi gerekiyor. Server ile client arasında gerçekleşen TCP-handshake olayını Wireshark üzerinden tespit edip sadece ilgili alanın (yakalanan paketlerin olduğu bölüm) resmini buraya ekleyiniz (Bütün yakalanan paketlerin resmini eklemeyiniz. Sadece TCP-Handshake olayının gerçekleştirildiği paketlerin olduğu bölümün resmini ekleyiniz).

2. Yukarıda belirtilen adrese tarayıcınız aracılığı ile erişmeye çalıştığınızda HTTP GET ve HTTP OK mesajlarını almanız gerekmektedir. HTTP GET mesajının gönderilmesinden HTTP OK yanıtı alınana kadar geçen süre nedir? (Erişim sürelerini tarih/saat formatında görebilmeniz için şu adımları Wireshark üzerinde uygulamalısınız:
    a. View > Time Display Format > Time-of-day)

3. İstek attığınız web sitenin, internet adresi nedir? Sizin bilgisayarınızın internet adresi nedir?

4. Açılan web sayfasında username ve password alanlarını doldurup login butonuna bastığınızda:
    a. Gönderilen istek GET metodu ile mi, POST metodu ile mi gönderilmiş?
    b. Yazmış olduğunuz username ve password bilgilerini paket detayları bölümünde listelenen bölümleri (Frame, Internet, Hypertext Transfer Protocol vb.) incelediğinizde görebiliyor musunuz? Görebiliyorsanız hangi alan üzerinden bu bilgiye eriştiğinizi belirtiniz.
    c. Eğer göndermiş olduğunuz username ve password bilgilerini paket detaylarında görebiliyorsanız, bu verinin şifrelenmiş olarak gönderilip gönderilmediğini belirtiniz. Eğer veriler şifreli olarak gönderildiyse bunun nedenini, şifreli olarak gönderilmediyse bunun nedeninin ne olduğunu kısaca belirtiniz.