BİLGİSAYAR AĞLARI DERSİ
WIRESHARK ÖDEVİ – 2 (DNS)

Bu ödevinizde DNS ile ilgili uygulamalar yapmanız, yakaladığınız bir ağ trafiği içerisindeki DNS paketleri ile ilgili bazı sorulara cevap vermeniz beklenmektedir.

1.Bölüm: `nslookup`

Yapılması gerekenler: (nslookup'ı nasıl kullanılıacağına dair araştırma yapmanız gerekir!)

1. `nslookup` komutunu kullanarak `iitb.ac.in` sunucusuna ait IP adresini bulunuz. Ekran görüntüsü ile gösteriniz.
2. `iitb.ac.in` sunucusuna ait güvenilir (authorative) DNS sunucularını elde etmek için nslookup sorgusunu gerekli parametreler ile yeniden çalıştırınız. Kaç farklı güvenilir DNS sunucusundan bilgi aldınız? Bu sunucuların IP adresleri nelerdir? Ekran görüntüsü ile gösteriniz.

2.Bölüm: Wireshark

Yapılması gerekenler:

- `ipconfig` komutu ile bilgisayarınıza ait IP adresini bulunuz. (MacOS: `ifconfig`)
- Bilgisayarınızdaki DNS önbelleğini temizleyiniz.
  - (Windows: `ipconfig /flushdns`
  - MacOS: `sudo killall -HUP mDNSResponder`)
- İstediğiniz bir internet tarayıcısını açarak önbelleğini temizleyiniz.
- Wireshark programını yönetici olarak çalıştırınız. Paket yakalama işlemini başlatınız.
- İnternet tarayıcısında `www.ietf.org` adresini ziyaret ediniz. Paket yakalama işlemini durdurarak yakalanmış paketlerin bulunduğu dosyayı kaydediniz. (Ör. 11111111111.pcapng)
- Görüntüleme filtresi (display filter) kısmına "ip.addr == ***.**.***.**" şeklinde, 1.soruda elde ettiğiniz IP adresini yazarak yakalanmış paketleri filtreleyiniz.

Yakalanmış paketleri içeren dosyadaki bilgilere göre aşağıdaki soruları cevaplandırınız.

1. DNS sorgu (query) ve cevap (response) mesajlarını bulunuz. Bu mesajlar TCP veya UDP protokollerinden hangisi ile gönderilmiştir? Ekran görüntüsü ile gösteriniz.
2. DNS sorgu mesajının port numarası nedir? Ekran görüntüsü ile gösteriniz.
3. DNS cevap mesajının port numarası nedir? Ekran görüntüsü ile gösteriniz.
4. DNS sorgu mesajını inceleyiniz. Bu sorgu mesajı herhangi bir cevap (answer) içermekte midir? İçeriyorsa bu cevabın içeriği nedir? Ekran görüntüsü ile gösteriniz.
5. DNS cevap mesajını inceleyiniz. Kaç tane cevap (answer) içermektedir? Bu cevapların her birinin içeriği nedir? Ekran görüntüsü ile gösteriniz.

Ödev gönderimi: Öğrenci ve ödev numarasını içerecek şekilde isimlendirilmiş, cevaplarınızın bulunduğu pdf dosyası (Ör: 11111111111_Odev2.pdf) ile yakaladığınız paketleri içeren dosyayı (Ör: 1111111111_Odev2.pcapng), sıkıştırarak tek bir dosya elde ediniz. Sıkıştırılmış dosyayı aynı şekilde (Ör: 1111111111_Odev2.zip) isimlendirerek son teslim vaktinden önce uzaktan eğitim sistemine yükleyiniz. Başka kaynaklardan gönderilen ve vaktinde gönderilmeyen ödevler değerlendirilmeyecektir.

Kopya Çekme Durumu

Kopya çekilmesine karşın sıfır tolerans politikamız vardır. Kopya çekenler üniversite yönetmeliğine göre cezalandırılacaktır.

Kopya Politikası: Öğrenciler/Gruplar kavramları kendi aralarında veya öğretim elemanı veya yardımcıları ile tartışabilirler. Ancak asıl işin yapılması söz konusu olduğunda, bunun sadece öğrenci/grup tarafından yapılması gerekir. Çözümünüzü yazmaya veya yazmaya başladığınızda, yalnız çalışmalısınız. Başka bir deyişle, doğrudan bir başkasından metin kopyalıyorsanız - ister dosyaları kopyalıyor, ister başka birinin notlarından yazıyor ya da onlar dikte ederken yazıyorsanız - kopya çekiyorsunuz demektir (daha kesin olmak gerekirse, intihal yapıyorsunuz anlamına gelir). Bu, kaynağın bir sınıf arkadaşı, eski bir öğrenci, bir web sitesi, çöpte bulunan bir program listesi veya herhangi bir şey olup olmadığına bakılmaksızın doğrudur. Ayrıca, programın küçük bir bölümünde bile intihal yapmak kopya çekmek anlamına gelir. Ayrıca, yazmadığınız bir kodla başlayıp, kendi kodunuz gibi görünecek şekilde değiştirmekte kopya çekmektir. Başkasının aldatmasına yardım etmek de aldatma sayılır. Programınızı açıkta bırakmak veya oturumu kapatmadan bir bilgisayardan ayrılmak, böylece programlarınızı kopyalamaya açık bırakmak, duruma göre kopya teşkil edebilir. Sonuç olarak, sizi kesinlikle kopya çekme suçlamalarına açık bırakacağından, başkalarının programlarınızı kopyalamasını önlemeye her zaman özen göstermelisiniz. Kopya çekilme durumunu belirlemek için otomatik araçlarımız var. Kopya çeken taraflar disiplin cezasına çarptırılacaktır.