KARADENİZ TEKNİK ÜNİVERSİTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
BİLGİSAYAR AĞLARI LABORATUARI

Wireshark ile Ağ Paket Analizi

❖ Deney Hazırlığı

1. Deney Ubuntu işletim sistemi üzerinde gerçekleştirilecektir. Deney ortamı ile ilgili diğer bilgiler Ek'te (son sayfada) verilmiştir.
2. Deneyde kullanılacak kaynak kodlar deney sayfasında verilmiştir. "Deneye Hazırlık" ve "Deney Soruları" kısımlarını dikkatlice okuyunuz, gerekli araştırmaları yapınız ve deneye hazır geliniz. Deney sırasında föy içerisinde verilen konularla ilgili bilginiz ölçülecektir. Yetersiz ve ilgisiz olanlar deneye alınmayacak veya çıkarılacaktır.
3. Deneyde; örneğin ARP protokolü ile ilgili ezber tanım cevapları vermeniz değil protokollerin çalışma mantıklarını kavramanız istenmektedir. Deneye föy içerisinde bilmeniz istenen (ARP, HTTP, TCP) protokollerin işleyişlerini bilerek geliniz.
4. Deney sırasında ilgili bölümlerde detaylıca verilen paket formatları üzerinde Wireshark ile paket yakalamamanız, analiz ve çözümlemeleri yapmanız istenecektir. Bunun dışında raw TCP paketleri üzerinde değişiklik yaparak Wireshark üzerinde gözlemlemeniz istenecektir. Kod düzenlemelerini gedit, Atom editörleri ile yapılabilir. Deney masalarında gibi metin editörleri kurulu olacaktır. Deney sırasında bu konularda bilgi verilmeyecektir, sizin bilmeniz istenmektedir. C kodlarının derlenmesi ve çalıştırılması ile ilgili hatırlatıcı bilgiler Ek I'de (son sayfa) verilmiştir.
5. Hazırlık ile ilgili sorularınızı cmyilmaz@ktu.edu.tr adresi elektronik posta ile iletebilirsiniz.

❖ Deney Tasarım ve Uygulanışı

1. Hazırlık soruları ile deneye hazırlık seviyesi ölçülecek. Deneye hazır olmayan ve ilgisiz olanlar deneyden çıkarılacaktır.
2. Deneyde; (1) föy içerisinde verilen ağ protokolleri ve paketler üzerinde ağ paket analizi (Deney Uygulaması [1, 2 ve 3] başlıklı uygulamalar), paket filtreleme vb. yapmanız, (2) raw TCP paketleri üzerinde basit değişiklikler yapmanız ve oluşan yeni paketleri Wireshark ortamında incelemeniz (Deney Uygulaması-4 başlıklı uygulama) istenecektir. Gerekli kaynak kodlar ve diğer açıklamalar föy içerisinde verilmiştir.

1. Giriş

Bu deneyde, Wireshark programı ile TCP/IP temelli ağlarda belirli seviyede detaylı paket ve protokol analizi gerçekleştirilecektir.

2. Ağ Paket Analizi ve Kullanım Alanları

2.1. Ağ Paket Analizi

TCP/IP günümüzde ağ üzerinde iletişim için en sık kullanılan protokol kümesidir ve bu kurallar dizisinde iletişim sayısal bilgi paketleri ve alt protokoller ile sağlanır. Bu nedenle sağlam ve güvenilir veri aktarımı için aktarılan bu paket ve protokollerin yapı ve içeriklerinin detaylı incelenebilmesi gerekir. Ağ paket analizi de temelinde bu amaçla yöneliktir ve basitçe herhangi bir ağ arayüzüne (ethernet vb.) gelen ve giden paket ve protokollerin incelenmesine olanak sağlar. Ağ paket analizi (network/packet sniffing) sniffer olarak adlandırılan araçlar ile gerçekleştirilir. Deneyde, belirli seviyede detaylı paket ve protokol analizine olanak sağlayan Wireshark ile ağ paket analizi yapılacaktır.

Deney Hazırlığı: Temel ağ kavramları, TCP/IP protokol kümesi, paket ve protokol kavramlarının neler olduğunu bildiğiniz varsayılacaktır. Varsa eksiklerinizi tamamlayarak deneye geliniz.

3. Wireshark Ağ Paket Analizi Yazılımı

3.1. Wireshark

Wireshark (eski adıyla Ethereal olarak bilinir), temelinde bir ağ paket ve protokol analiz (sniffer) yazılımdır ve bir bilgisayar ağı üzerinde akan trafiğin yakalanması ve etkileşimli olarak içeriğinin irdelenmesi/gözlenmesine olanak sağlamaktadır. Amacına yönelik zengin özellikleri ile günümüzde kendi türünün en yaygın kullanılan ve fayda sağlayan araçlarından bir tanesidir. Özellikleri ile ilgili detaylar Bölüm 3.2'de, örnek bazı kullanım senaryoları ise Bölüm 3.3'te verilmiştir. Uçbirim sürümü olan Tshark'da aynı amaç için kullanılabilir.

3.2. Wireshark'ın Özellikleri

- Windows, OS X, Linux ve Unix platformlarda kullanılabilir, açık kaynak kodlu ve GPL lisanslı bir yazılımdır
- Gerçek zamanlı analiz, çok kıstasta filtreleme ve aramaya olanak sağlar (sadece HTTP paketlerini göster vb.)
- Ağ üzerinde gerçek zamanlı ve etkileşimli paket yakalamaya olanak sağlar, çok çeşitte ağ protokolünü destekler
- tcpdump/WinDump ve diğer bazı paket yakalama programlar ile kaydedilmiş paketleri açabilir
- Paketleri detaylı protokol bilgileri ile gösterebilir
- Yakalanan paketleri daha sonra tekrar incelemek için kaydedebilir, farklı formatlarda dışa aktarıma izin verir
- İyi derecede grafik arayüzüne sahiptir, paketlerin renklendirilmesi vb. ile görsel olarak kolay paket analizine olanak sağlar

3.3. Örnek Kullanımlar Alanları

1. Ağ uzman ve yöneticileri tarafından ağ trafiğinin incelenmesi, sorunlarının irdelenmesi/çözümlenmesi
2. Ağ/bilgi güvenliği mühendisleri tarafından güvenlik problemlerinin incelenmesi
3. Uygulama geliştiriciler tarafından protokol implementasyonlarının debug edilmesi. Örneğin bir Apache web sunucusunun debug edilerek sunucu veya uygulama kaynaklı bugların belirlenerek sunucu hatası ve olabilecek aksamaların önüne geçilmesi, veya ağ kart ve yazılımının hataların belirlenmesi, analiz edilmesi vb.
4. Bu deneyde olduğu gibi ağ paket ve protokollerinin öğrenilmesi

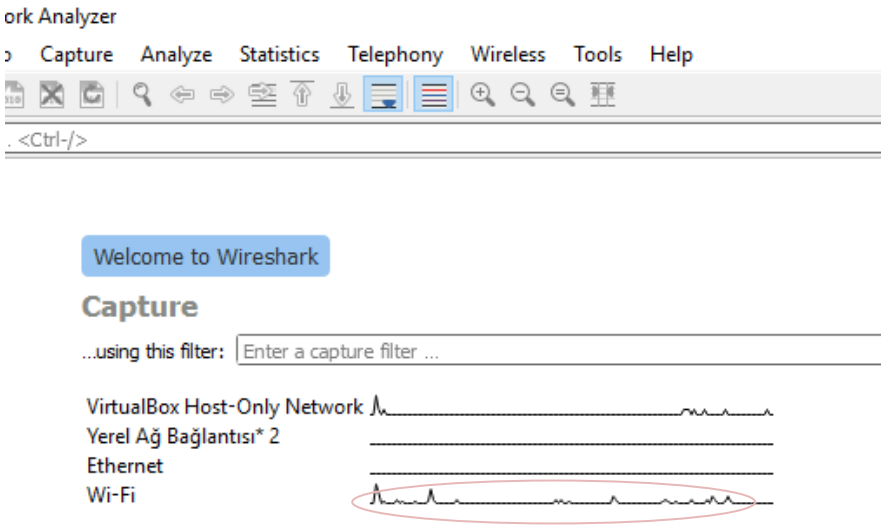
3.4. Kurulum

Windows: https://www.wireshark.org/download.html adresinden indirilebilir ve standart kurulum adımları uygulanarak kurulum işlemi gerçekleştirilebilir. Linux: apt-get komut satırı aracında *sudo apt-get install wireshark* komutu ile gerekli paketlerin edinilmesi ve yükleme işlemi gerçekleştirilebilir. Deneyde Linux ortamında Ubuntu işletim siteminde paket yakalama ve analizi gerçekleştirilecektir. Detay için Ek-I'e (son sayfa) bakınız.

3.5. Wireshark ile Paket Yakalama

Wireshark Windows ve Linux ortamlarında standart program adımları ile çalıştırılabilir. Yazılım çalıştırıldığında aşağıdaki ekran (Şekil 1) ile karşılaşılır. Burada öncelikle paketleri yakalanacak ağ arayüzü seçilir ve daha sonra Start düğmesine tıklanarak (veya Ctrl+E tuş kombinasyonu) paket yakalama işlemi başlar. Wireshark ortamında ağ arayüzleri ile ilgili detaylı bilgiye bu bağlantıyı kullanarak erişebilirsiniz. Uygulamayı çalıştırdığınızda aşağıdaki gibi ağ arayüzleri listelenecektir. Dikkat edecek olursanız Wi-Fi arayüzü üzerinden veri aktarımı yapılmaktadır. Bu arayüze çift tıklarsanız paket yakalamaya başlayacaktır. Deneyde ethernet arayüzü üzerinden paket dinleme gerçekleştirilecektir. Araç çubuğunda *Capture->Options* yolunu izleyerek arayüzleri detaylı görebilirsiniz. Eski (GTK+) kullanıcı arayüzü Wireshark Legacy'de görünüm biraz daha farklıdır, ancak, benzer şekilde arayüz seçme ve paket yakalama gerçekleştirilebilirsiniz.

Deney Hazırlığı: Bu dokümanda Wireshark'ın detaylı kullanım bilgisi verilmeyecektir. İnternet üzerinde kullanımı ile ilgili birçok dijital kaynak bulunmaktadır. Deneye gelmeden bu kaynaklardan faydalanarak Wireshark yazılım aracını kullanabilir seviyede hazır olmanız gerekmektedir. İlerleyen bölümlerde çeşitli protokoller üzerinde kullanım ve filtreleme işlemleri kısmen anlatılmıştır.



Şekil 1. Ağ arayüz seçimi

4. Çeşitli Protokoller Üzerinde Ağ Paket Analizleri

4.1. Adres Çözümleme Protokolü (ARP) Paket Analizi

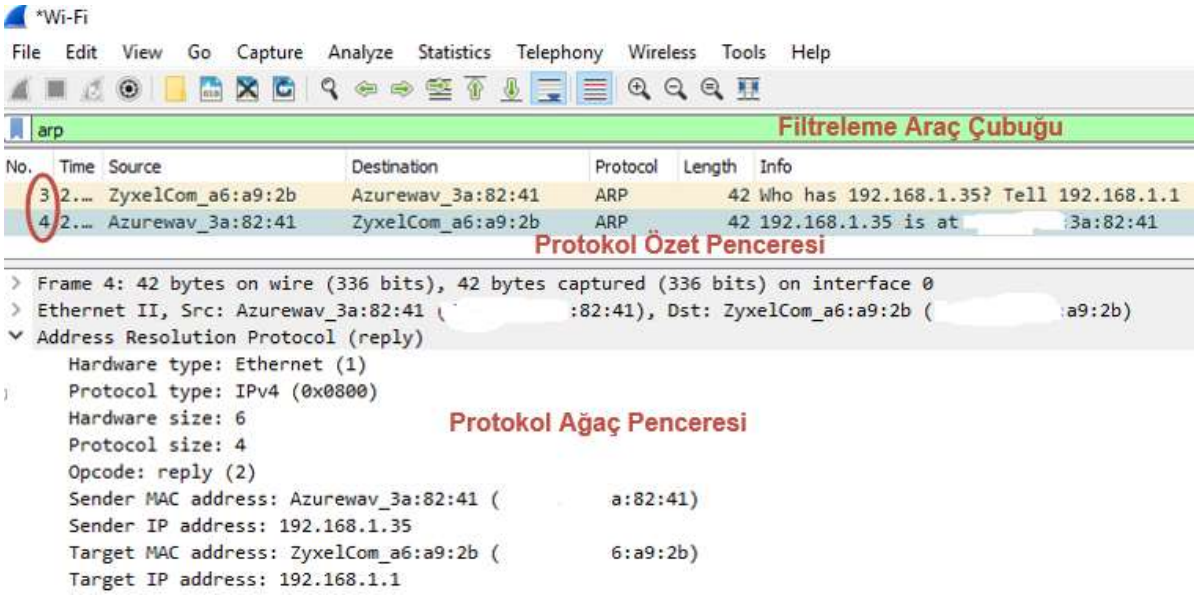
4.1.1. ARP Nedir?

Yerel ağ içerisindeki cihazların haberleşebilmeleri cihazların fiziksel adresleri ile yapılır. Bu amaçla basit olarak ağ üzerindeki cihazlar birbirlerine paket göndermek için fiziksel adreslerini edinmeleri gerekir ve bu edinim işlemi IP'si bilinen bir cihazın fiziksel adresinin öğrenilmesini sağlayan ARP protokolü ile gerçekleştirilir. (Örneğin, MAC (Ethernet, Media Access Control Adresses) adresleri bir fiziksel adrestir ve yerel ağlardaki cihazların birbirlerine veri paketi göndermeleri için bir ağ adresi olarak kullanılır. 48 bit olan bu adresler her ağ arayüzü için tekildir.

4.1.2. Wireshark ile ARP Paket Analizi

Deney Hazırlığı: Aşağıda detaylı biçimde anlatılan ARP paket analiz işlemlerini deneye gelmeden gerçekleştiriniz, soruları cevaplayınız. Deney hazırlığı kısmında sizden paketler üzerinde anlatmanız istenecektir.

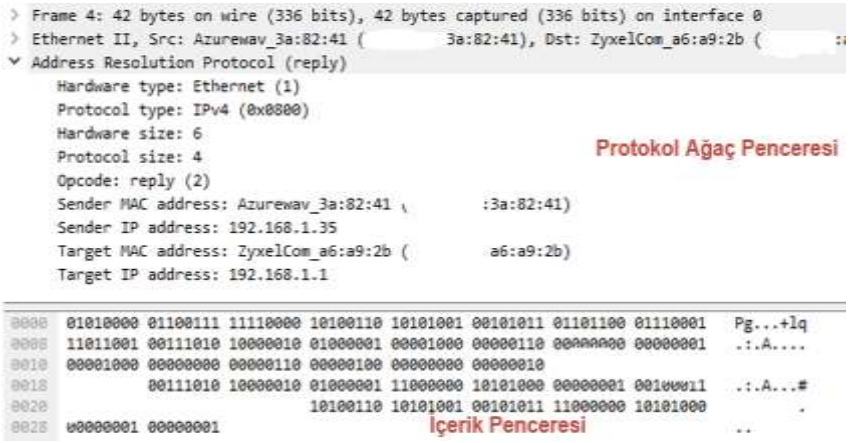
Bu alt bölümde, Wireshark ile bilgisayar ağ arayüzü dinlenmiş ve ARP paketleri Filtreleme Çubuğuna yazılan *"arp"* (tırnaksız) parametresi ile filtrelenmiş ve aşağıda verilen örnek paketler yakalanmıştır. (Filtreleme işlemleri Başlık 5'te kısaca anlatılmıştır.)



Şekil 2. Yakalanan örnek bir ARP Paket çifti (istek ve cevap)

Yukarıda yakalanan 3 ve 4 numaralı paketler ARP protokolünü anlamak için yeterlidir. 3 numaralı paket bir istek (sorgu) paketi, 4 numaralı paket ise bir cevap paketidir. Detaylı incelenirse, 192.168.18.1 IP adresli cihaz tüm yerel ağa yayın yapacak şekilde 3 numaralı ARP sorgu paketini yollayarak, 192.168.18.35 IP adresine sahip cihazın fiziksel adresini sormaktadır. Bu sorgu paketini alan 192.168.1.35 IP adresli cihaz ARP sorgusunun kendisine geldiğini IP adres eşleşmesinden anlamakta ve içine kendi MAC adresini yazarak ARP cevap paketi hazırlayarak ve istekte bulunan cihaza gönderir Böylece IP adresinden fiziksel adrese dönüşüm işlemi gerçekleştirilmiştir.

Paketlerin katman temelli yapısı ve içerikleri aşağıda gösterildiği (Şekil 3) gibi detaylı görüntülenebilir. Protokol ağaç ve protokol içerik pencereleri bu amaçla kullanılabilir. Bu pencerenin amacı protokol özet penceresinde seçili olan paket içeriğini katmanlı ağaç yapısı şeklinde göstermektir. Veri görüntüleme penceresinde ise seçili paket veya alanın bilgilerini onaltılık veya bit düzeyinde gösterir.



Şekil 3. Örnek bir ARP paket içeriği

Standart bir ARP paketinin yapısına bakılacak olunursa (Tablo 1) ise kaynak ve hedef cihazlara ait fiziksel ve IP adresleri, donanım türü, protokol türü, donanım adres uzunluğu, protokol adres uzunluğu ve işlem türüne (opcode) ait değerler yer almaktadır.

Fiziksel Katman Başlığı	
Donanım Tipi	Protokol Türü
Donanım Adres Uzunluğu	Protokol Adres Uzunluğu
İşlem Türü Kodu	
Gönderici Donanım Adresi	
Gönderici IP Adresi	
Alıcı Donanım Adresi	
Alıcı IP Adresi	

Tablo 1. *Örnek bir ARP paket yapısı*

4.1.3. Deney Uygulaması 1- ARP Paket Analizi

Bu uygulamada, ARP dönüşümünü ağ üzerinde yakaladığınız herhangi bir istek ve cevap ARP paket çifti ile paket seviyesinde anlatmanız istenecektir. Paketleri yakalamanız için kullanabileceğiniz bir senaryo aşağıdaki gibidir. Bunun dışında farklı yöntemlerde kullanabilirsiniz. Önemli olan ARP dönüşümünün nasıl yapıldığını protokol ve paket seviyesine anlama ve yorumlayabilmenizdir.

1. Wireshark ile paket yakalamaya başlayın.
2. IP & fiziksel adres eşleşmeleri bellek üzerinde tutulduğundan gerekmedikçe ARP sorgusu yapılmaz. Bu nedenle bellek temizlenerek ARP isteği oluşturulmalıdır. Windows ortamda: komut satırında <*arp –d*> komutu ile ARP ön belleğini temizleyebilirsiniz (Öncesinde <*arp –a*> ile mevcut ARP kayıtlarını görebilirsiniz).
3. Herhangi bir adrese ping atın. Örneğin: <*ping 192.168.1.2*> komutu ile verilen IP adresine ping atabilirsiniz. Detay için web üzerinden araştırma yapınız.
4. Belirli bir süre bekledikten sonra Wireshark ile yakalanan paketlere ARP filtresi uygulayın.
5. Yakalanan paketlerden adres dönüşümü yapan bir ARP paket çiftinden (request/istek ve reply/cevap) faydalanarak aşağıdaki tablo tabloyu doldurun.

İstek Paketi	
Ethernet Paketi	

Cevap Paketi	
Ethernet Paketi	

6. Yakalan paketlerden faydalanarak aşağıdaki soruları cevaplayın.

   6.1. İstek ve cevap paketlerinde hangi opcode değerleri kullanılır, paket başlıklarının (header) boyutu nedir?

6.2. ARP katman kaçta çalışır?
6.3. Bir ARP istek paketinde hedef fiziksel adres değeri ne olur, neden?
6.4. ARP cevap (reply) paketleri istek (request) paketleri gibi broadcast mi yapılır, yapılmazsa neden? İstek paketleri neden broadcast edilir, IP zaten biliniyorsa, IP ile direk gönderilemez mi?
6.5. IP adresi varken, neden fiziksel adres kullanılıyor? Ağ geçidi vb. bir cihazın IP adresini hiç iletişime geçmeden makine nasıl biliyor?

4.2. HTTP Paket Analizi

4.2.1. HTTP Nedir?

HTTP (Hypertext Transfer Protocol) Dünya Çağında Ağ (World Wide Web, WWW) üzerinde web sayfaları ile bilgi (metin, görüntü, ses, video vb. çoklu ortam dosyaları) alış verişi yapmaya olanak sağlayan basit ama güçlü bir standart kurallar kümesidir. Basitçe bir istemci (örn. web tarayıcısı) ve sunucu (örn. web sunucusu) arasında taşınacak bilginin nasıl kodlanacağı ve aktarılacağına dair kuralları düzenler. TCP/IP'de uygulama katmanında yer alan bir protokoldür.

Örnek bir HTTP istek paketi

Tarayıcı ile http://ceng.ktu.edu.tr/ adresine bağlanmak istediğinde tarayıcının sunucuya göndereceği örnek bir istek paketi şu şekilde olacaktır:

```
GET / HTTP/1.1
Host: ceng.ktu.edu.tr
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
```

Örnek bir HTTP cevap paketi

Sunucu tarafından tarayıcıya cevap olarak gönderilen paket içeriğinin bir kısmı şu şekilde olacaktır:

```
HTTP/1.1 200 OK
Date: Mon, 16 Feb 2015 17:39:03 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3769
Keep-Alive: timeout=5
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-9
```

Deney Hazırlığı: HTTP çalışma prensibi, paket yapısını araştırarak deneye geliniz. Bu adresteki kaynaktan faydalanabilirsiniz.

4.2.2. Deney Uygulaması 2- HTTP Paket Analizi

Deneyin bu kısmında ağ üzerinde yakalanan HTTP paketleri incelenecek, temel çalışma prensipleri tartışılacak, anlatmanız istenecek, paket filtreleme vb. işlemlerle HTTP ile ilgili bazı soruları cevaplandırmanız istenecektir. Wireshark ile HTTP paket trafiğini incelemek için yapılabilecek örnek bir senaryo adımları sırası ile aşağıdaki gibidir.

1. Wireshark programını çalıştırın ve paket yakalamaya başlayın.
2. İnternet tarayıcısını çalıştırın ve herhangi bir web adresine bağlanın (yeterli paket trafiği oluşması için site üzerinde gezinin).
3. Yeterli miktarda paket yakaladıktan sonra paket yakalamayı durdurun.
4. Sadece HTTP paketlerinin görüntülenmesi için gerekli filtrelemeyi yapın.

Deney sırasında yukarıdaki adımlar gerçekleştirildikten sonra HTTP protokolünde istek ve cevap mekanizmasının nasıl çalıştığı hakkında konuşulacak ve yakalanan Http paketleri ile ilgili bazı soruları cevaplamanız istenecektir. Örnek bazı sorular şu şekildedir:

1. Tarayıcınız veya sunucu hangi HTTP sürümünü desteklemektedir?
2. Tarayıcınıza sunucu tarafından döndürülen durum kodları nelerdir?
   Diğer sorular deney sırasında verilecektir.

4.3. Paket Filtreleme

Deney Hazırlığı: Wireshark üzerinde örnek paket filtreleme işlemleri yaparak deneye geliniz.

Açıklama: Filtreleme çubuğunda herhangi bir filtre girdisi yapıldığında protokol özet penceresinde sadece filtrelenen paketler görünür. Bazı filtre ifadeleri ve açıklamaları şu şekildedir:

- *eeth.addr == 00:0b:6b:be:xx:xx > Gönderici veya alıcı fiziksel ethernet adresi 00:0b:6b:be:xx:xx olan paketleri listeler.*
- *tcp.port eq 25 or icmp > SMTP veya ICMP paketlerini listeler.*
- *http or dns >> HTTP veya DNS paketlerini listeler.*
- *ip.addr == 10.0.0.1 && ip.addr == 10.0.0.2 > Tanımlı iki IP adresi arasındaki paket trafik akışını listeler.*
- *port 53 > Sadece DNS trafiğini listeler.*
- *host www.ceng.ktu.edu.tr and not (port 80 or port 25) > Sunucudan gelen http ve SMTP dışındaki trafiği listeler.*
- *(tcp[0:2] > 1500 and tcp[0:2] < 1550) or (tcp[2:2] > 1500 and tcp[2:2] < 1550) > Belirli port değer aralığındaki paketleri listeler.*
- *link[0] != 0x80 > Beacon dışındaki WLAN trafiğini listeler.*

4.3.1. Deney Uygulaması 3 – Filtreleme İşlemleri

Deney uygulamasında özellikle HTTP ve diğer bazı protokoller üzerinde filtreleme işlemlerini gerçekleştirmeniz istenecektir. Sorular deney sırasında verilecektir.

4.4. Raw TCP Paketlerinin İncelenmesi

Deney Hazırlığı: Kaynak kodlar bu adreste verilen <raw_tcp_socket.c> dosyasında yer almaktadır. Kodları inceleyerek hazır bir şekilde deneye geliniz.

4.4.1. Deney Uygulaması 4 – Raw TCP Paketlerinin Analizi

Deney uygulamasında <raw_tcp_socket.c> dosyasında yer alan raw TCP paketi üzerinde değişiklik yapmanız, oluşan paketleri Wireshark ile yakalamanız ve analiz etmeniz istenecektir. Kodların derlenmesi ve çalıştırılması hakkında bilgi için Ek-I'e (son sayfa) bakınız.

4.5. Internet Kontrol Mesajı Protokolü (ICMP) Paket Analizi

ICMP paket analizi deney sonrasında boş zaman kalması durumunda gerçekleştirilecektir. Deney hazırlığında çalışmanıza gerek yoktur.

ICMP bir IP ağı içerisinde IP datagramların iletimi ile ilgili sorunların belirlenmesi için kullanılan bir protokoldür. Ping istemci arayüzü ile kolaylıkla ping atılabilir ve uçtan uca işlevsel bir IP yolunun olup olmadığı tespit edilebilir.

Deney Hazırlığı: ICMP protokolü hakkında bilgi sahibi olunuz.

4.3.1. Deney Uygulaması 5- ICMP Paket Analizi

Bulunduğunuz yerel ağdaki herhangi bir makineye ping atın ve oluşan ICMP paketleri ile ilgili aşağıdaki soruları cevaplayın.

1. Ping nedir, ne için kullanılır, ICMP protokolü temelde nasıl çalışır, açıklayınız.
2. Kaç adet ICMP paketi (istek ve cevap) oluştu?
3. Kaynak ve hedef cihazların IP adresleri nelerdir?
4. ICMP paketleri neden *kaynak* ve *hedef port numarası* içermez?
5. Siz tarafından gönderilen herhangi bir ICMP paketini inceleyin. Paketteki ICMP *type* ve *code number* değerleri nelerdir? Paketteki *checksum*, *sequence number* ve *identifier fields* değerleri ne için kullanılır, kaç bayt uzunluktadır?
6. Size gelen bir ICMP paketini inceleyin. Paketteki ICMP type ve code number değerleri nelerdir?
7. TCP/IP modeline göre hangi katmanda hangi protokol yer alır?

Deney Hazırlığı: Deneye gelmeden yakaladığınız paketler üzerinde örnek filtreleme işlemleri gerçekleştiriniz.

5. Deney Raporu

1. Deney raporuna deney sayfasında yer alan "Deney Raporu" doküman kapak dosyası olacak şekilde hazırlanacaktır. Raporlar grup olarak (veya istenirse bireysel) hazırlanacak ve bir hafta içerisinde Moodle platformu üzerinden teslim edilecektir. Deney rapor soruları Bölüm 5'te verilmiştir. Kopya raporları hazırlayan gruplar gerekli sorumluluğu üzerlerine almış sayılırlar. Raporu dikkatlice okuyunuz, gereksiz kısımları rapora yazmayınız.

5.1. Deney Rapor Soruları

UDP taşıma protokolü ile ilgili aşağıdaki soruları cevaplayınız. Makinenizin UDP paketleri üretmesi için *nslookup* komutunu kullanın. Bu komut ağınızın varsayılan DNS sunucusuna bir DNS sorgusu gönderir ve sorguladığınız alan adının IP adresini size yollar. Örneğin, komut satırından *nslookup printfriendly.com* komutunu koşarsanız, sözel ifadeyle *printfriendly.com alan adına sahip bilgisayarın IP adresini bana gönder* demiş olursunuz.

1. Wireshark ile paket yakalamaya başlayın.
2. Komut satırından nslookup ceng.ktu.edu.tr şeklinde bir DNS sorgusu koşun. *Not: İstemciler (bilgisayarlar) DNS adresleri DNS önbelleğinde tutarak, tekrar tekrar alan adı IP adresi dönüşümü yapmayı engellemek ve hızlı yapmak isterler. Bu denenle DNS önbelleğinde olmayan bir alan adını sorgulayın veya DNS önbelleğinizi temizleyin.*
3. Cevap IP adresi geldiğinde paket yakalamayı sonlandırın.
4. DNS paketlerini filtreleyin. *Filtrelenen paketlere bakacak olursanız taşıma katmanında UDP kullanıldığını göreceksiniz.*

Yakalanan paketler ile ilgili aşağıdaki soruları deney raporuna cevaplayın.

1. Bir paket seçin, UDP başlığı yapısı hangi alanlar var (source port vb.), yazınız. UDP için RFC 768 dokümanından da faydalanabilirsiniz. Paket formatı ve alanlar dokümanda da verilmiştir.
2. UDP için tanımlı protokol numarası nedir? (Cevap için IP başlık bilgisine bakın)
3. UDP başlık bilgisinin boyutu ne kadardır?
4. UDP başlık yapısında yer alan *length* alanındaki sayısal değer neyi ifade eder? Vereceğiniz cevabı yakaladığınız paket üzerinde hesaplayarak doğrulayın ve kısaca nasıl hesapladığınızı açıklayın.

9. Kaynaklar

1. *The Internet Engineering Task Force, https://www.ietf.org/.*
2. *Wireshark, http://www.wireshark.org/.*
3. *TCP/IP Ağlarda İleri Seviyede Paket Analizi, http://www.bga.com.tr/calismalar/tshark.pdf.*
4. *J.F. Kurose, K.W. Ross., Wireshark and ICMP, Computer Net. Lab., Computer Networking, A Top-down Approach.*
5. *http://www.cse.chalmers.se/edu/year/2012/course/EDA343/Assignments/Assignment1/wireshark_lab.ppd, Wireshark ve HTTP.*
6. *Capturing Traffic Wireshark, http://www.comm.utoronto.ca/~jorg/teaching/ucc/handouts/. Lab1-UCC2012-Wireshark.pdf.*
7. *Uluşahin U., Basa G., Wireshark Kullanım Kılavuzu.*
8. *Ayvazoğlu Ç., Wireshark - İTÜ BİDB Ağ Grubu .*
9. *https://github.com/rbaron/raw_tcp_socket/blob/master/raw_tcp_socket.c*

EK-I

Wireshark Kurulumu

Wireshark arayüzü Linux ve Windows platformlarda aynıdır.

Windows ortamında https://www.wireshark.org/download.html adresinden indirilebilir ve standart kurulum adımları uygulanarak kurulum işlemi gerçekleştirilebilir. Gerekirse yönetici olarak çalıştırılmalıdır.

Linux ortamında *apt-get* komut satırı aracında *sudo apt-get install wireshark* komutu ile gerekli paketlerin edinilmesi ve yükleme işlemi gerçekleştirilebilir. Yüklemem işleminden sonra Wireshark ile paket yapabilmek için aşağıdaki komutların gerekli sistem izinleri için koşulması gerekmektedir.

- sudo dpkg-reconfigure wireshark-common
- sudo adduser $USER wireshark

Raw TCP Paketlerinin Derlenmesi ve Koşulması

Kod düzenlemelerini gedit, Atom editörleri ile düzenleyebilirsiniz. Deney masalarında gibi metin editörleri kurulu olacaktır. Deney sırasında bu konularda bilgi verilmeyecektir, sizin bilmeniz istenmektedir.
C kodlarının gcc ile derlenmesi ve çalıştırılması aşağıdaki gibidir. Bu konuda eksiklikler varsa deneye eksiklikleri tamamlayarak gelinmesi gerekmektedir. Kaynak kodlar deney sayfasında verilmiştir.

Derleme: `$ gcc girdi_kaynak_kod_dosyasi.c -o yürütülebilir_cikti_dosyasi`
Koşma: `$ ./yürütülebilir_cikti_dosyasi`