HAFTA 2

BÖLÜM A

1. Mekanik ve Altyapı

Karışık modu açmak ağdaki kendi dışında diğer paket alışverişlerinide görmemizi sağlar. Mod kapalıysa sadece üç tip kabı kabul eder; kendi ağ paketi, herkesin ulaşabileceği ağdaki paketler, önceden bağlandığın özel abonelik gruplar.

Hub ile Switch arasındaki farkı ses seviyesi diye düşünebiliriz.Hub eskiden kullanılan ağdaki her şeyi herkesin duyduğu bir ağ iletişimi , Switch ise sadece alıcı ve verici arasında oluşan ses sistemi ağdaki diğerleri duyamaz. Saldırganın kullanacağı yol ARP Poisoning (Alıcı ve vericiyi kandırmak) .

Log dosyasında sadece işlemin gerçekleştiğine dair bir bilgilendirmedir, detay göremezsin. Wiresharkın kaydettiği Pcap dosyasında ise detaylı bir bilgilendirme vardır. Hasta kayıt sistemi gibi düşünebilirsin koridordaki hastaların gördüğü içerdeki hastanın isim ,soy isim yani Log ama doktor içerideki hastanın her bilgisini görebilir yani Pcap. Herhangi bir durumda kesin delil olarak Pcap geçerlidir çünkü daha detaylı bilgi sahibidir.

2. Protokol Anatomisi

3-Way Handshake (Üçlü El Sıkışma) durumunu biriyle yeni tanışıyormuşsun gibi açıklayacağım .Sen ilk olarak elini uzatarak kendini tanıtırsın işte bu SYN yani kendine ait olan ulaşım yolu , karşı tarafta elini uzatır ve seninkini tutarak kendini tanıtır bu da SYN-ACK yani karşı tarafta kendi ulaşım yolunu sana göstererek tanışalım der. Son olarak ellerinizi sıkarak anlaşırsınız ACK yani onaylama, tanışma tamam gibi düşünebiliriz.

TCP ile UDP ‘yi nakliyeci gibi düşünebilriz.Aralarındaki fark TCP güvenilir ,paketin varış yerine ulaştığından emin olur ayrıca yavaştır bu yüzden banka hesaplarında kullanılır.UDP daha hızlı bir nakliyecidir paketin içinde kırılacak eşya var mı pek umursamaz yani yoldaki kayıplar onu ilgilendirmez. Paket kaybı olduğunda TCP kaybı bulmaya çalışır ama UDP ilgilenmez.

Sıra numarası alıcının herhangi bir gönderimde eksik, sonradan gelen paketleri birleştirirken karıştırmaması için önemlidir. Eğer 5.paket 3.paketten daha önce ulaşırsa alıcı onu Tampon Bellek (Buffer) odasına alır diğer paketlerde geldiğinde hepsini sırasına göre hizalar ve gönderenin ilettiği mesajı ortaya çıkarır.

3. Kimlik ve Adresleme

IP adresi medeni durumunuz gibidir, MAC adresi ise sizin TC Kimlik numarası gibi özeldir. Düşün birini arıyorsun elinde sadece medeni durumu var ‘bekar’ onu bulman zor olur bu yüzden ondan TC Kimlik numarasını da istiyorsun böylece ARP sorunu kolayca çözüyor.

DHCP adresi (DORA Süreci) kiralık ev arama süreci gibi düşünebiliriz.İlk önce emlakçıya gidersin (KEŞFET), sana istediğin şekildeki evleri gösterir (TEKLİF), aynı evlere başka emlakçılarda da bakarsın hoşuna gideni tutarsın (TALEP), emlakçı evin anahtarını sana verir (ONAY) .

DNS bilgisayarın telefon rehberi gibidir.Taracıya google.com yazdığımızda bilgisayar onu rehberde arar bulamazsa geçmiş aramalara bakar , yine bulamazsa Root (Kök Sunucusu) ,TLD Sunucusuna sorar sonunda Yetkili sunucu veya DNS Response soruya cevap verir.

4. Şifreleme ve Kör Noktalar

Wireshark ile şifreli bir paket yakaladığımızda kullanıcı adı ve şifreyi göremiyoruz. Şifreli kısımlardan geriye IP adresi, port numarası,SNI,sertifika belgeleri,davranış analizi kalır.

HTTPS bağlantısında bilgisayarın ile sunucu arasında şifreli bir iletişimdir .Ortadaki adamın iletişimdeki konuşmaya ulaşması için şifreyi çözmesi gerekir ama şifreyi çözemediğinden kendince yeni şifre yapar, bilgisayarı ya da sunucuyu taklit ederek sahte sertifika yani şifreyi biliyormuş gibi davranır ve konuşmaya ulaşır.

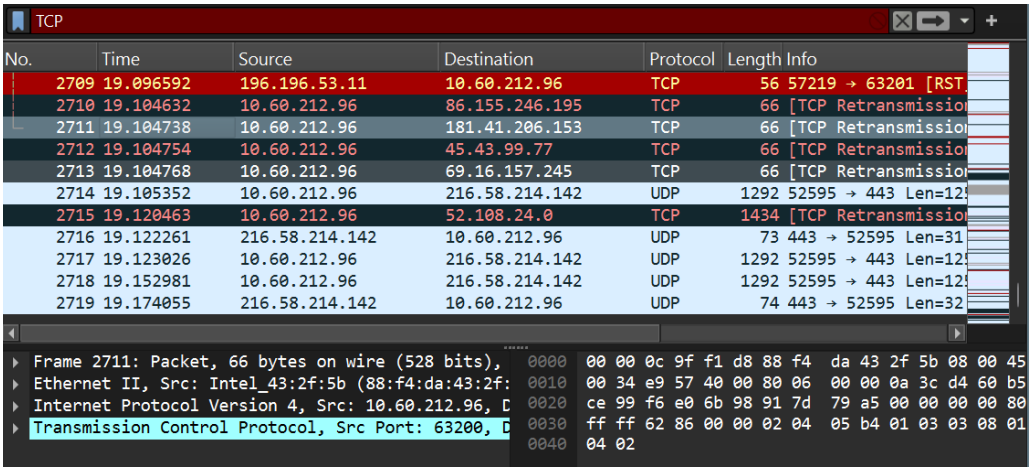
5. Saldırı İmzaları

Normal iletişimde sırayla SYN, SYN-ACK, ACK yaparak kapıyı açıp içeri girersin, Taramada ise SYN gönderip karşı taraftan SYN-ACK alınca kapının açık olduğunu anlayıp iletişimi keser bu da Wireshark'ta yarım kalmış kırmızı bağlantılara neden olur. Normal iletişimde aynı anda max iki kapı kullanır ama Taramada aynı anda birsürü kapı kullandığını görürsün.Normal iletimde sistemsel nefes alma boşlukları var ama Taramada öyle bir şey yok Wireshark'ta arka arkaya bir sürü paket dizisi görürsün.

Hizmet Reddi (DoS) oteldeki bütün odaları rezerve etmen ama sonrasında odalara rezerve sahiplerinin gelmemesi tam o sıra başka müşterilerin oda istediğini ama boş odanın kalmadığını söylemen gibi bir şeydir.TCP bağlantısı kurulana kadar bağlantı bilgilerini Backlog Queue belleğinde tutar ama bellekte ayrılan yer sınırlıdır . Ayrılan yer dolunca yarım açık bağlantı kuyruğu kilitlenir.

BÖLÜM B

1. Arayüz ve Renkler



Frame : en dış katman , fiziksel katman paketin içinde kaç bit olduğu, hangi saniye yakalandığı, hangi ağ arayüzünden geçtiğini söyler.

Ethernet II : Veri bağlantısı katmanı paketin hangi bilgisayarın ağ kartından çıktığını ve hangi fiziksel kapıya gittiğini gösterir.

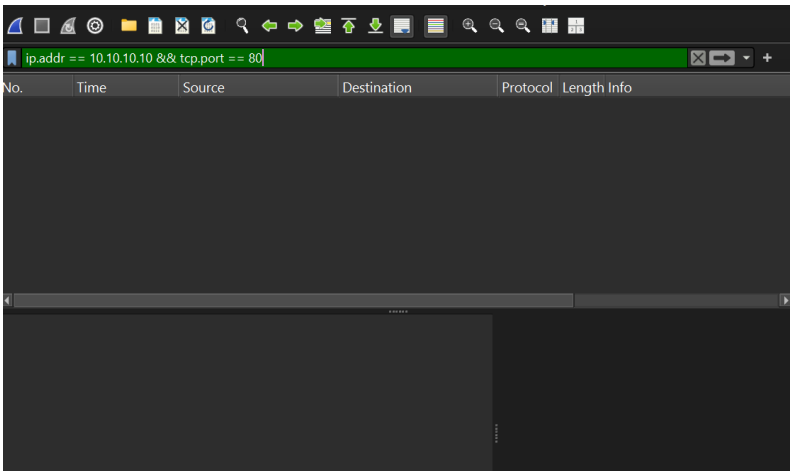
Internet Protocol : Ağ katmanı , paketin IP adresini gösterir.

Transmission Control Protocol : Taşıma katmanı , paketin hangi portu kullandığını, paketlerin doğru sırada olup olmadığını kontrol eder.

Wireshark'ta arka planı siyah olan satır gördüğünde mantığı TCP protokolüyle ilgili sıkıntısı olduğu anlamına gelir. Yani paketlerin yolda kaybolduğunu, sırasının karıştığını veya gecikme yaşandığını

söyler. Kırmızı satırlar ise bağlantının tam kapatılmadığı anlamına gelir.İletişimin aniden dur komutu aldığı ya da kaba bir şekilde kapatıldığı manasına gelir.

2. Filtreleme Sanatı (Görev 5: Yakalananları Filtrelemek)



Filtre kesme : ip.addr == 10.10.10.10 && tcp.port == 80

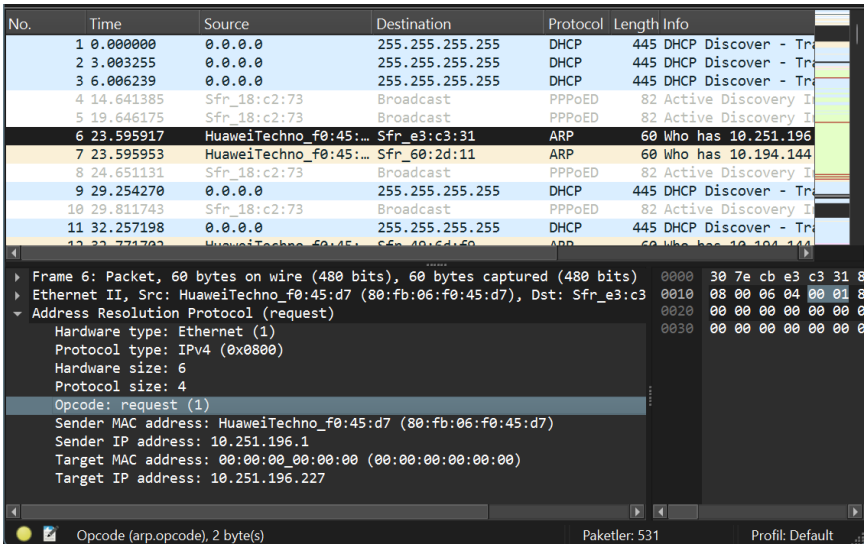
3. OSI ile Paket İlişkisi (Görev 6: Paket Diseksiyonu)

Ethernet II alt başlığı Source (Kaynak) ve Detination (Hedef) adresleri MAC'tir. OSI modelinin 2.katmanı Data Link Layer içersindedir.

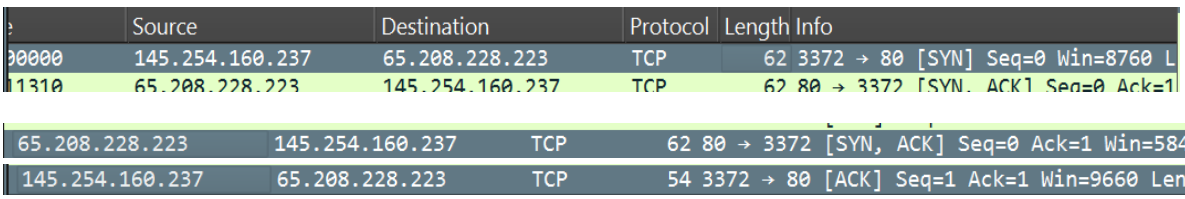
4. ARP Trafiği (Görev 7: ARP Trafiği)

Opcode 1 ağa gönderilen soru mesajıdır yani istektir. IP adresinin sahibini sorar.

Opcode 2 ise soruya verilen resmi mesajdır yani cevaptır. IP adresinin sahibi bulunur.

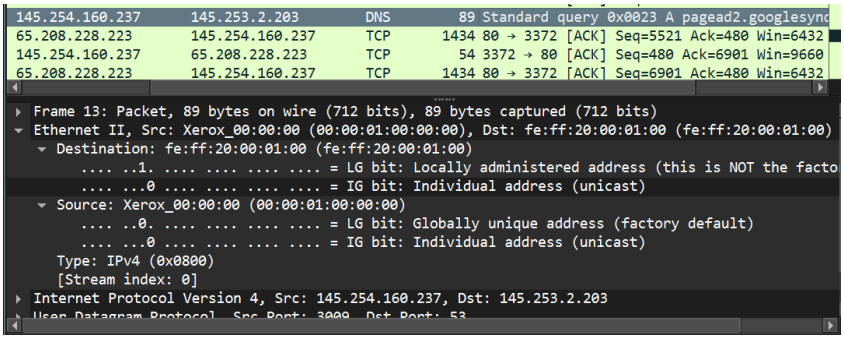


5. TCP El Sıkışması (Görev 9: TCP Trafiği)

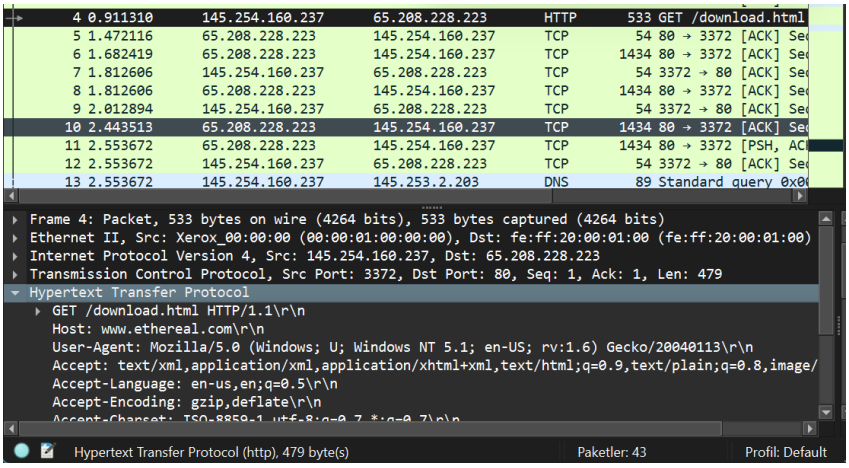


6. DNS Sorguları (Görev 10: DNS Trafiği)

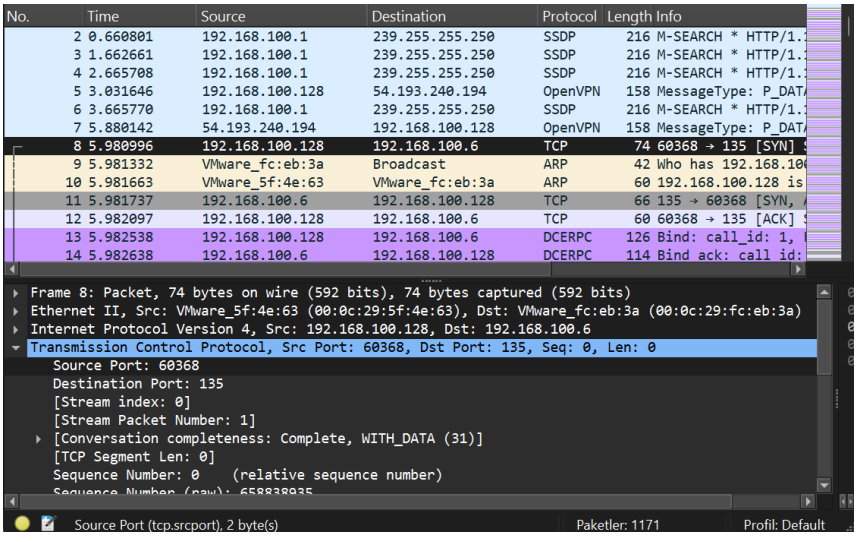
Sorgu paketi UDP protokolu ile gider.



7. HTTP vs HTTPS (Görev 11 ve 12)



8. Saldırı Analizi (Görev 13: İstismarı Analiz Etmek)



Siyah satıra bakıldığında 192.168.100.128 IP adresine sahip cihazın saldırgan olduğunu düşünüyorum. Her şüpheli durum kırmızı satır olmak zorunda değildir, aslında zararlı olduğunu renginden değil davranışından anlıyoruz.

BÖLÜM D

1. Kırmızı Çizgi: Etik ve Hukuk (TCK Kapsamı)

Hukuki boyut olarak madde 243: Bilişim Sistemine Girme bir yıla kadar hapis veya adli para cezası verilir. Madde 132:Haberleşmenin Gizliliğini İhlal bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Madde 244:Sistemi Engelleme, Bozma,Verileri Yok Etme veya Değiştirmedende hukuki ceza alınabilir.Yetkili olmayan bir ağda karışık mod açmamalıyız,IDS yüzünden izlenebilirliğiniz artar, meslekte güvensiz birine dönüşürsünüz, sabıka kaydınız çalışmanıza engel olur.

2. Veri Yorumlama

Dosya uzantısı sadece kullanıcılar için , içerik işletim sistemi ve programlar içindir. Magic bytes değiştirilemez. Dosya uzantısı hangi uygulamada çalışacağını belli eder ,değiştirilince farklı uygulamada çalışır ama Magic bytes değişince yapısı değişir bilgisayar yorumlama hatası verebilir, dosya açılmayabilir.

3. Düzenli ve Sessizlik

Siber dünyada yaptığınız ufak şeyler bile dijital ayak izi bırakabiliyormuş onu farkettim. Sessiz bir şekilde sızmak bu yüzden imkansız. Mavi takım için gürültü kavramı iz sürmek için güzel bir fırsat böylece daha kolay saldırganı bulabiliriz.