HAFTA 2: Ağ Adli Analizi ve Derin Paket İnceleme (DPI)

Görev 2: Packet Detective Raporu (Proje Ödevi)

Bölüm A: Teori ve İstihbarat (Research & Logic)

1. Mekanik ve Altyapı: "Ağı Dinlemek"

Promiscuous Mode (Gelişigüzel Mod): Wireshark'ı başlattığımızda neden bu modu aktif ederiz? Eğer bu mod kapalı olsaydı, ağ kartımız (NIC) sadece hangi paketleri kabul ederdi?

Normalde ağ kartımız işlemciyi yormamak için sadece kendisini ilgilendiren paketleri alır ve bu şekilde çalışır ama promiscuous modu aktif edildiğinde ise ağ kartı ağ kanalında gelen bütün paketleri yakala hepsini görmek istiyorum der. Bu mod aktif edilmediğinde ise genel herkesi ilgilendiren paketler, bilgisayarımızda üye olduğumuz kanallardan gelen paketler ve bir de bizim mac adresimize tanımlanmış paketleri alırız.

Hub vs. Switch Farkı: Eski "Hub" cihazlarında tüm trafiği görmek kolaydı. Ancak modern "Switch"ler trafiği izole eder. Bir Switch ortamında başkasının trafiğini (örneğin Ali'nin Veli'ye attığı mesajı) görebilmek için saldırganlar hangi manipülasyonu (ARP Poisoning / Port Mirroring) yapmak zorundadır?

Evet eski sistemlerde hublar adeta tüm binaya yayın yapardı bir mesaj paketini iletirken .Yani wireshark ı açan herhangi bir kişi mesajın içeriğini rahatlıkla okuyabillirdi. Ama şimdi kullanılan switchler ise mesaj iletirken adeta bir postacı gibi davranır kapıya kadar gelir ve kapının altından sessizce size mesajı iletir. Bu mesajın içeriğni öğrenmek isteyen kişiler için ise artık işleri biraz daha zorlaştırır. Yeni yöntemle ARP Poisoning dediğimiz yöntemle Man-in-the-Middle saldırıları yapar , bu saldırı switch i kandırır . Ali'ye gider derki ben Veli'nin MAC adresine sahibim ,Veli'ye ise ben Ali'nin MAC adresine sahbim diyerek gelen paketleri alır içeriğini görür ve aynı şekilde gönderilen kişiye teslim eder. Port Mirrorin bir saldırı değil yönetici özellğidir. Bunu biz yönetici olarak herhangi bir porttaki trafiğin kopyasını isteyerek alırız .Bu sorun giderme aşamasında gereklidir. Saldırganlar bunu ancak yönetici panelinin şifresini kırarlarsa yapabilirler.

Pcap vs. Log: Bir Firewall'un ürettiği "Log" dosyası ile Wireshark'ın kaydettiği "Pcap" dosyası arasındaki temel fark nedir? Bir siber olay müdahalesinde (Incident Response) hangisi "kesin delil" sayılır, neden?

Pcap dosyası kesin delil sayılır. Çünkü firewall log u bir kapı defteri gibidir. Sadece deftere geleni geçeni yazar bir de defterde yazılan zararlı olarak yazılmış olanları içeri almaz . Onun haricinde ise içeri giren paketlerin içinde zararlı yazılım olup olmadığını bilemez . Siber güvenlik analisti buna bakarak saldırının başarılı olup plmadığını anlayamaz ama Pcap dosyası bir ağ trafiğinin tamamen kopyasını çeker paketin içinde ne olup olmadığını siber güvenlik analisti görebilir . Bu sayede saldırının başarılı olup olmadığını anlayabilir. Bu yüzden Pcap dosyası bir kesin delil sayılır.

2. Protokol Anatomisi: "Dijital El Sıkışma"

3-Way Handshake (Üçlü El Sıkışma): TCP bağlantısı kurulurken gerçekleşen SYN -> SYN-ACK -> ACK trafiğini bir telefon görüşmesi analojisi gibi bir örnek ile açıklayın.

1. Adım: SYN (Senkronize Et / Başlat)

- **Venom:** Telsizin tuşuna basarsın.
  - *"Merkez, burası Venom. Beni duyuyor musun? Tamam."*
  - *(Burada sadece sen istek gönderdin. Karşı tarafın orada olup olmadığını veya seni duyup duymadığını henüz bilmiyorsun.)*

2. Adım: SYN - ACK (Senkronize Et + Onayla)

- **Merkez (Sunucu):** Telsizi açar.
  - **ACK (Onay):** *"Venom, seni net duyuyorum."* (Senin çağrını aldı).
  - **SYN (Başlat):** *"Peki sen beni duyuyor musun? Operasyona hazır mısın? Tamam."*

3. Adım: ACK (Onayla ve Bitir)

- **Venom:**
  - *"Anlaşıldı Merkez, seni duyuyorum. Dosyaları göndermeye başlıyorum."*
  - *(İşte bu son "Anlaşıldı" lafından sonra bağlantı resmen kurulur.)*

Dikkat edersek bağlantı başlatma ve senkronizasyon aşamalarında SYN kullandık , onaylama aşamalarında ise ACK kullandık. TCP bu yolla bağlantının güvenli olup olmadığına karar verir. Eğer herhangi bir aşamada bir problem olsaydı bağlantı kurulamazdı.

Sequence Number (Sıra Numarası): Paketlerin üzerine neden numara yazılır? 5. paket, 3. paketten önce gelirse bilgisayar bunu nasıl düzeltir?

İnternet ortamında herhangi bir veri paketler halinde karşı tarafa gönderili her paketin üzerinde bir numara yazar . Eğer ki her paket numaralandırılmasaydı , bir anlam karmşası ortaya çıkabilirdi örnek vereyim : Ali mehmet'ten daha arkadaş canlısıdır=> Mehmet canlısıdır Ali'den arkadaş . Bu yüzden her pakete bir numara atanır. Diyelim ki herhangi bir paket zamanından erken gelseydi ve daha öncesinde gelmesi gereken paket gelmemiş paket olsaydı nolurdu ? Önce gelen paket Buffer yani bekletme odasına alınır. sırası geldiğinde Reorderin uygulanarak sıranın yeniden dizilmesini sağlayıp karşı tarafa (uygulma vb.) teslim ederdi.

3. Kimlik ve Adresleme: "Postacı Kapıyı Çalar"

ARP Protokolü (Who has?): Bilgisayarlar IP adresiyle (Örn: 192.168.1.1) haberleşmek ister ama fiziksel olarak MAC adresine ihtiyaç duyarlar. ARP protokolü bu sorunu nasıl çözer? (Broadcast mantığı).

Elinde ağdaki IP si X olan kişiye ait bir mesajın var ama mesajı verdiğin kişiye ait olduğunu söyleyen MAC adresini doğrulaman gerekir . Yoksa kime ait olduğunu bilemezsin . Bu durumda ARP (Address Resolution Protocol) burada devreye girer. X IP'si kime aittir der ve burada senin cihazın bana ait der MAC adresini söyle der ve sen de söylersin . Bundan sonraki seferlerde ARP ın bağırmasına gerek yoktur. Çünkü ARP tablosuna senin MAC ini kaydeder ve bundan sonra sana MAC A der, bundan sonraki seferlerde direkt MAC A kim ,der ve saldırganlar bu kısımda devreye girer. Benim der (bilgisayarımız buna inanır ve veriyi gönderir) ve gönderilen veriyi alır .

DHCP (DORA Süreci): Bir bilgisayar ağa ilk bağlandığında IP adresi yoktur. IP almak için gerçekleştirdiği Discover -> Offer -> Request -> Acknowledge (DORA) sürecini kısaca özetleyin.

D (Discover): "Alooo! Bana acil IP lazım, kimse yok mu?" (Bilgisayar bağırır)

O (Offer): " Sunucu (DHCP) bunu duyar ve al kardeşim, 192.168.1.5 boşta, işini görür mü?" (Sunucu"DHCP" teklif eder)

R (Request): "Tamamdır, bu 1.5 numara benim olsun, tuttum!" (Bilgisayar ister)

A (Acknowledge): "Anlaştık, hayırlı olsun. 24 saatliğine kullanabilirsin. Ama süre bitmeden gelip yenile der.

DNS (İnternetin Rehberi): Tarayıcıya google.com yazdığımızda arkada neler döner? Bilgisayar bu ismin IP karşılığını bulmak için kime sorar? (DNS Query / Response).

google.com yazdığımızda bilgisayarımız ilk başta kendi önbelleğini (Local Cache) kontrol eder, Eğer burada yoksa DNS çözümleyiciye gider (bilgisayarımızın asistanı gibi düşünebiliriz.) O da sırasıyla Kök sunucuya (Root Server)->TLD sunucusu (Top Level Domain -".com")->Yetkili Sunucu (Authoritative Server-"google.com") giderek google.com un IP adresini öğrenip bize getirir tabiki bunlar milisaniyeler içerisinde gerçekleşir.

4. Şifreleme ve Kör Noktalar: "Sır Perdesi"

HTTPS ve Şifreleme: Günümüzde trafiğin %90'ı TLS/SSL (HTTPS) ile şifrelidir. Wireshark ile şifreli bir paketi yakaladığımızda "Kullanıcı Adı ve Şifreyi" görebilir miyiz?

Göremiyorsak, bir analist olarak elimizde hangi veriler kalır? (Meta-data: IP, Port, SNI vb.)

HTTPS (TLS/SSL) ile şifreleme bir mektubu kargoya verirken sağlam bir kasaya koyup vermek gibidir. Wireshark ile gideceği Portu, siteyi yani adresi görebiliriz ama içeriğini göremeyiz . Nitekim kasanın üstünde de adres yazılıdır. Ama içini kargocu göremez. Ayrıca dijital kimliğini (sertfika, yani kime ait olduğu) de görebiliriz .

Man-in-the-Middle (Ortadaki Adam): Şifreli trafiği çözmek (decryption) için saldırganlar neden araya girip sahte sertifika sunmaya çalışır?

Sertifikalar aslında dijital kimliklerdir ve içlerinde Public Key (Açık Anahtar) taşırlar. Saldırgan trafiği yakalasa bile elinde bu anahtar olmadığı için şifreyi çözemez . İşte bu noktada Sahte sertfika devreye girer. Saldırganlar Senin trafiği gönderdiğin sunucunun serfikasını taklit eden ben senin ulaşmak istediğin sunucuyum mesajı veren bir şekilde taklit bir sertfika anahtarı oluşturur ve iki tane şifreli tünel kurar . Senden aldığı veriyi okuyup orjinal anahtarlarla tekrar senin gönderdiğin sunucuya gönderir.

5. Saldırı İmzaları: "Suçluyu Tanımak"

Port Taraması (Port Scanning): Bir saldırganın "Açık kapı var mı?" diye kontrol etmesi (Scanning) ile normal bir bağlantı isteği arasında Wireshark'ta nasıl bir fark görürüz? (Örn: Sürekli SYN gönderip, cevabı beklemeden hattı kapatmak).

Wireshark'ta bu ikisi arasındaki fark, "Kapıyı çalıp içeri girmek" ile "Zile basıp kaçmak" arasındaki fark gibidir, "Sürekli SYN gönderip, cevabı beklemeden hattı kapatmak " buna ise SYN Scan (Half-Open

Scan / Yarı Açık Tarama) denir. Noramal bir bağlatıda olanlar : SYN->ACK-SYN->ACK ama SYN Scan : SYN-> ACK-SYN->RST(Reset) "Sadece bakıyorum anlamında bir yoklamadır ."

Denial of Service (DoS): Bir sunucuya saniyede 100.000 adet SYN paketi gelmesi (SYN Flood) sistemi nasıl kilitler? (Yarım açık bağlantı kuyruğu).

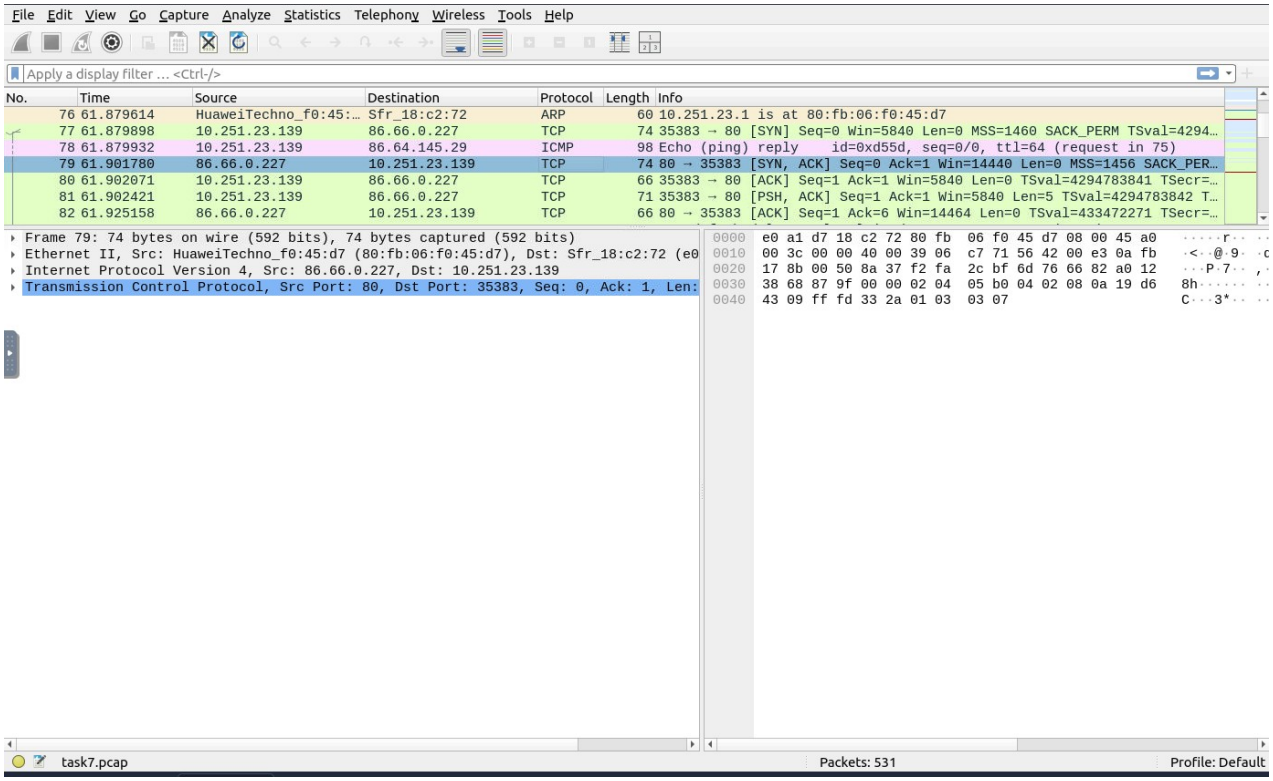
Şöyle açıklayalım 10.000 kişilik yeri boş yeri olan restorana 100000 tane rezervasyon geldiğinde dolar değil mi ? Ama rezervasyonların büyük bir kısmının sahte olduğunu düşünün bu sayede gerçek misafirler de restorana giremez . Çünkü rezerve edilmiş olarak gözüküyordur bunun gibi düşünelim. Normal bir süreçte sistem SYN_ACK-SYN_SYN şeklinde ilerlerken bu saldırı esnasında süreç : SYN_ACK-SYN_sessizlik (yani ACK yok). Her sunucunun bir kapasitesi vardır . Dolunca girişlere izin vermez. 10000 lik kapasitede 10000 istek gelirse kapasitenin aşıldığını düşünüp 10000' den sonrakileri içeri almaz.

Bölüm B: Saha Eğitimi ve Araç Hakimiyeti (TryHackMe - Wireshark 101)

1. Arayüz ve Renkler (Task 3: Wireshark Overview)

Soru: "Packet Details" paneli, OSI katmanlarını (Layer 2, 3, 4) hiyerarşik olarak gösterir. Bir pakete tıkladığınızda Frame, Ethernet II, Internet Protocol ve Transmission Control Protocol başlıklarını gördüğünüz bir ekran

görüntüsü ekleyin ve açıklayın.



Frame: Layer 1 (Fiziksel) bilgilerini içerir.

Ethernet II: Layer 2 (Veri Bağlantı) bilgilerini, özellikle MAC adreslerini gösterir.

Internet Protocol Version 4: Layer 3 (Ağ) bilgilerini, yani Kaynak ve Hedef IP adreslerini gösterir.

Transmission Control Protocol: Layer 4 (Taşıma) bilgilerini, kaynak/hedef portları ve bayrakları (Flags) gösterir."

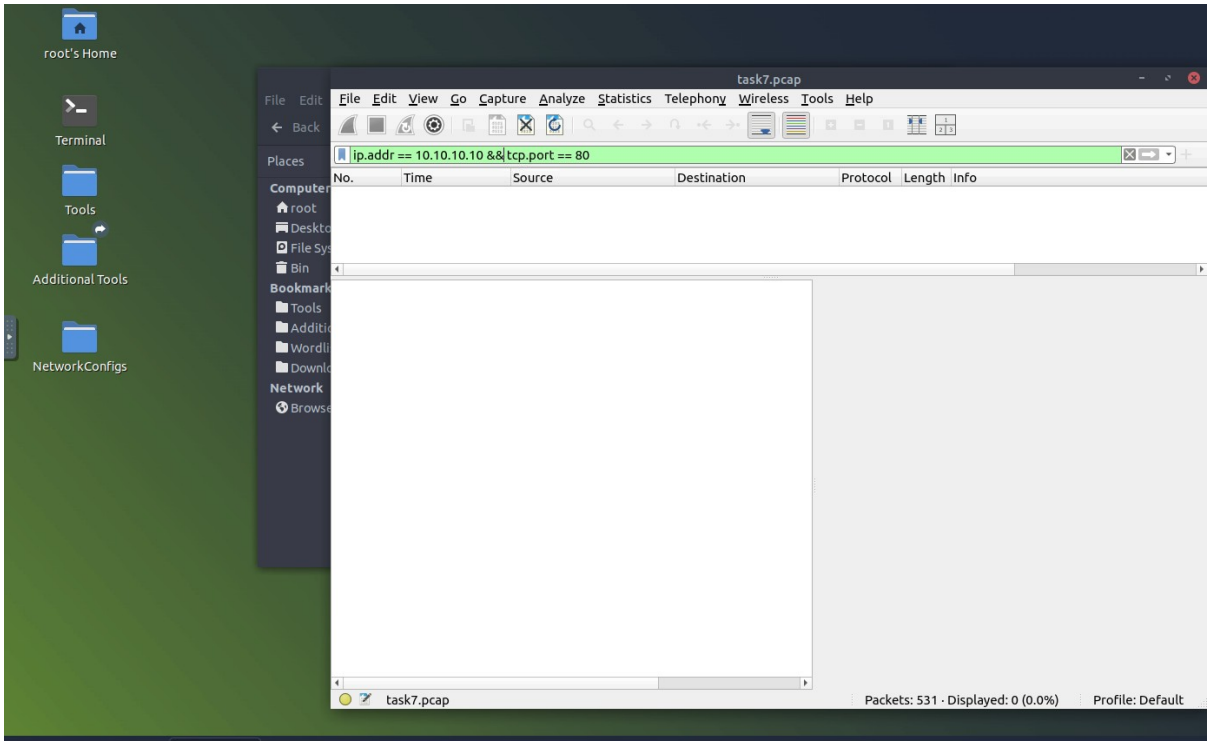
Soru: Wireshark'ta bazı paketler Kırmızı veya Siyah arka planla gösterilir (Bad TCP vb.). Bu renklerin analist için anlamı nedir? (Kısaca açıklayın).

Siyah Arka Plan / Kırmızı Yazı (TCP Errors): İletişim kopukluğu veya veri kaybı var. olduğunu gösterir ve analist için anlamı ağda tıkanıklık , gecikme (lag) veya paket kaybı olduğunu gösterir.

Kırmızı Arka Plan / Beyaz veya Sarı Yazı (Critical) : Bağlantının aniden kesildiğini veya paketin bozuk olduğunu haber vermek için kullanılır. Analist için ise bir port scanning , güvenlik duvarı engellemesi veya sistemsel bir hata olduğunu gösterir.

2. Filtreleme Sanatı (Task 5: Filtering Captures)

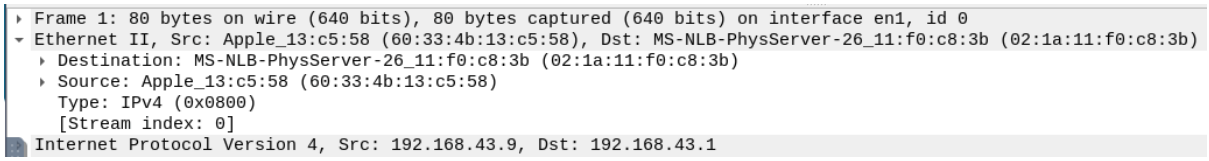
Görev: Sadece IP adresi 10.10.10.10 olan VE (AND) portu 80 olan paketleri görmek istiyorsunuz. Yazmanız gereken filtre komutu nedir?



Wireshark filtre çubuğuna ip.addr == 10.10.10.10 && tcp.port == 80 komutu girilmiştir. Ekran görüntüsünde görüldüğü üzere, filtre çubuğunun arka planının Yeşil renk alması, girilen filtrenin sözdiziminin (syntax) doğru ve geçerli olduğunu kanıtlar. Onun haricinde task5.pcapng dosyasını bulamadım bu yüzden bu IP adresine sahip olan işlemlerin ağ trafiğine tam olarak ulaşamadım.

3. OSI ile Paket İlişkisi (Task 6: Packet Dissection)

Soru: Packet Details panelinde Ethernet II başlığını genişletin. Burada gördüğünüz "Source" ve "Destination" adresleri, OSI modelinin hangi katmanına (Layer) aittir? (IP mi, MAC mi?)



MAC Adresleridir ve Layer 2'ye (Data Link / Veri Bağlantı Katmanı) aittir. Donanımların fiziksel MAC adresleri bu katmanda bulunur.

4. ARP Trafiği (Task 7: ARP Traffic) Ağdaki "Kimlik Sorma" mekanizması.

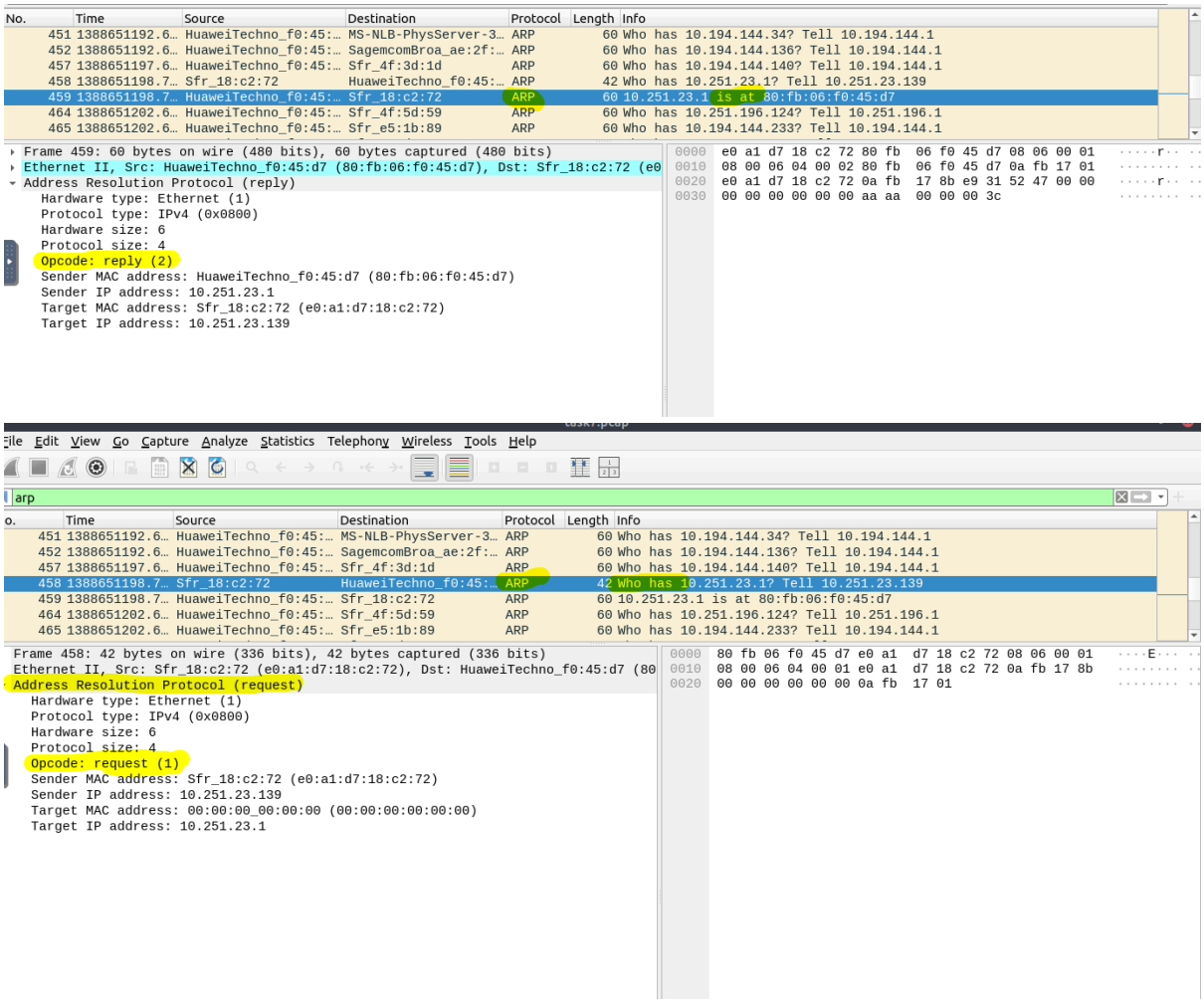
Soru: ARP protokolü iki tür mesaj içerir: "Opcode 1" ve "Opcode 2".

Opcode 1 ne anlama gelir? (Request/Reply?)

Opcode 2 ne anlama gelir?

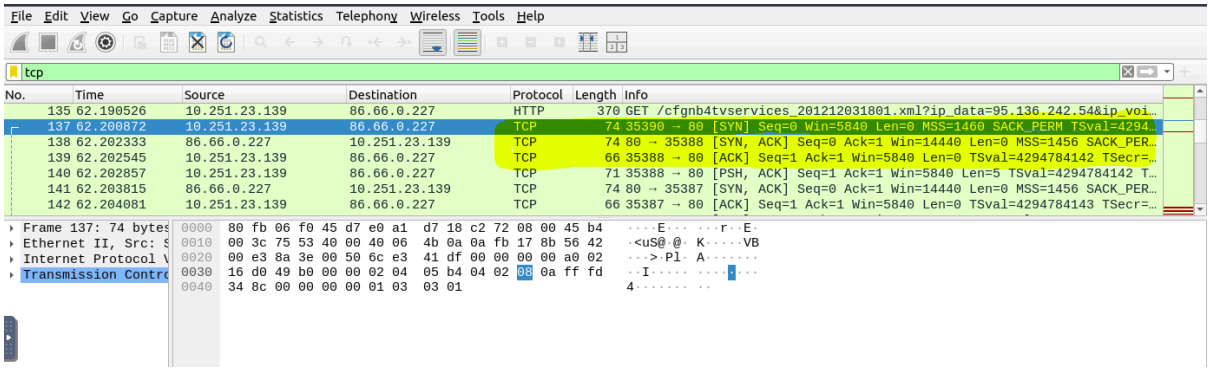
Opcode 1: ARP Request (İstek) , mesajın sahibini bulurken kullandığı sistemdir . Cihazın ağdaki IP sinin mesajın iletileceği cihazı bulmak için ilk aşamadır. ARP ağda X IP sine sahip cihaz kimin diye bağırdığı aşamadır.

Opcode 2: ARP Reply (Cevap) Opcode 1 aşamasında duyuru yapan ARP Request'e cihazın yanıt verdiği aşamadır. Yani o IP bana ait , der cihaz bu aşamada.



5. TCP El Sıkışması (Task 9: TCP Traffic)

Görev: Trafik içinde 3-Way Handshake (SYN -> SYN/ACK -> ACK) işlemini bulun.



1-)Paket 137 [SYN]: İstemci bağlantıyı başlatır .

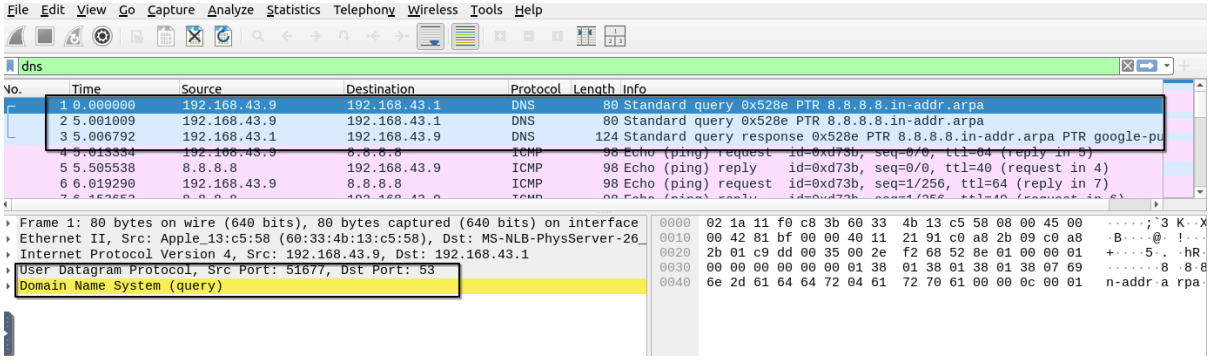
2-)Paket 138 [SYN, ACK]: Sunucu isteği onaylar (ACK) ve kendi başlatma isteğini gönderir(SYN)

3-)Paket 139 [ACK]: İstemci son onayı verir ve bağlantı kurulur . Bağlantı kurulum aşamalarının başarıyla tamamlandığını gösterir.

6. DNS Sorguları (Task 10: DNS Traffic)

Soru: Bir bilgisayar google.com'a gitmek istediğinde önce DNS sunucusuna sorar.

Sorgu paketi (Query) hangi protokolle gider? (TCP/UDP?)



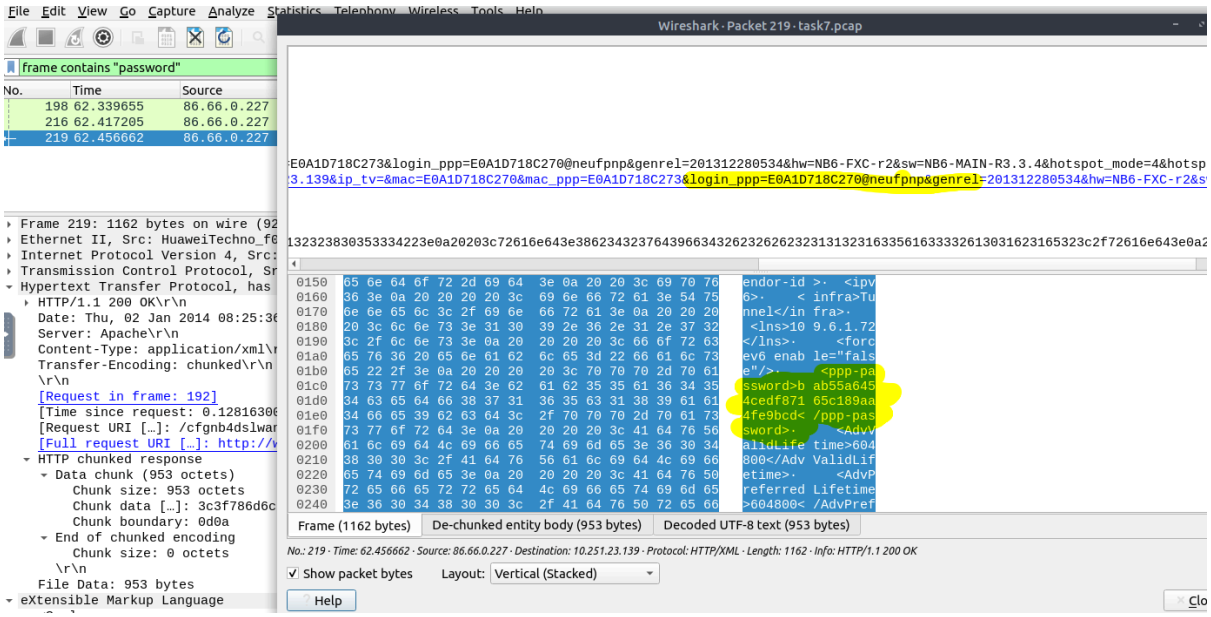
Protokol: DNS sorguları, Transport Layer (Taşıma Katmanı) seviyesinde User Datagram Protocol (UDP) kullanmaktadır. DNS sorguları hız önemli olduğu için TCP yerine UDP kullanıyor.

Sorgu Tipi: Paketin 'Domain Name System (query)' başlığı ve Info kısmındaki 'Standard query' ibaresi, bunun bir DNS isim çözümleme isteği olduğunu kanıtlar.

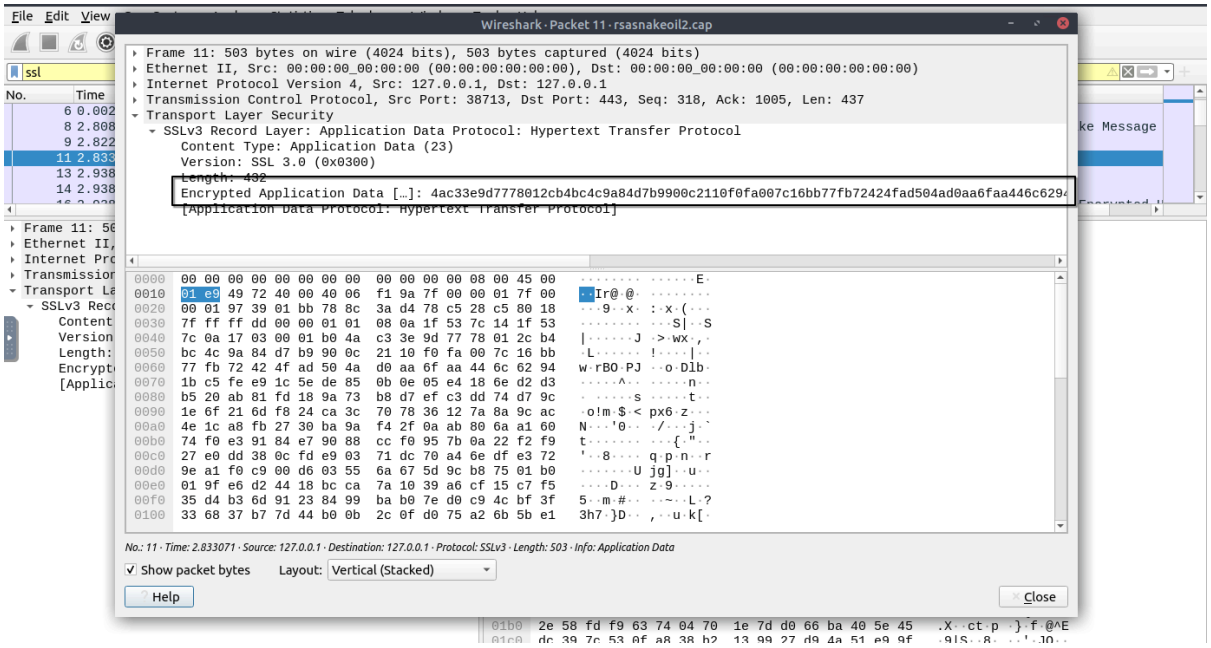
Hedef Port: Trafik, standart DNS portu olan 53 numaralı porta gitmektedir.

7. HTTP vs HTTPS (Task 11 & 12)

HTTP Analizi: Task 11'deki pcap dosyasında bir POST isteği (Login işlemi) yapılmıştır. Paket detaylarına bakarak gönderilen kullanıcı adı ve şifreyi açık metin (Cleartext) olarak bulun ve ekran görüntüsünü ekleyin.



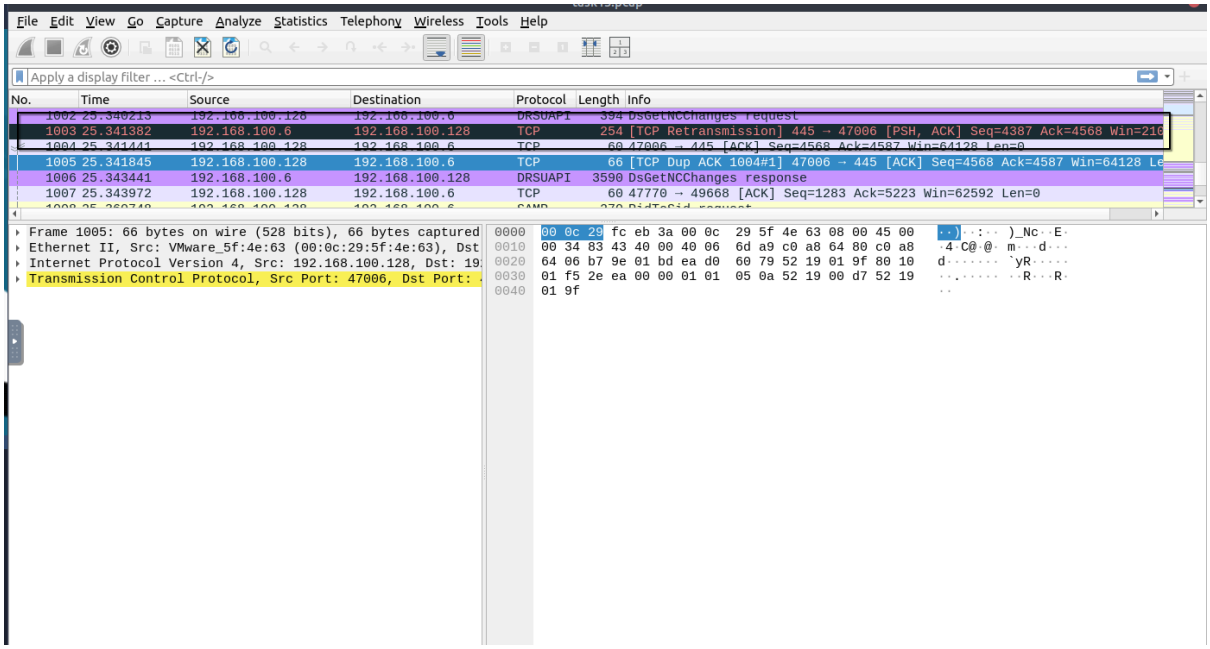
HTTPS Analizi: Task 12'de şifreli trafik vardır. Burada "Application Data" kısmına baktığınızda anlamlı bir metin görüyor musunuz? Gördüğünüzü (veya göremediğinizi) ekran görüntüsüyle kanıtlayın.



HTTPS trafiği şifreli olduğu için 'Application Data' içeriği okunabilir metin (Plaintext) yerine şifrelenmiş (Encrypted) karmaşık verilerden oluşmaktadır. Bu nedenle kullanıcı adı, şifre veya sayfa içeriği görüntülenememektedir.

8. Saldırı Analizi (Task 13: Analyzing Exploit)

Soru: Bu görevde saldırgan, sisteme sızmak için bir "Exploit" kullanıyor. Wireshark bu tür şüpheli durumları genellikle kırmızı ile işaretler veya uyarı verir.



Görselde, 1003 numaralı pakette görülen 'TCP Retransmission' uyarısı (Kırmızı/Siyah renk kodlaması), gerçekleştirilen saldırının ağ trafiğinde yarattığı anormalliği göstermektedir. Ayrıca 1002 numaralı paketteki 'DsGetNCChanges Request' isteği, saldırganın Active Directory verilerini çekmeye çalıştığı bir DCSync saldırısı gerçekleştirdiğini kanıtlar.

🕵️ BÖLÜM C: Vaka Analizi (Evidence Files)

Göreviniz: evidence01.pcap dosyasını analiz ederek aşağıdaki soruları yanıtlayın:

1-)Suç Ortağı: Ann'in mesajlaştığı kişinin kullanıcı adı (Buddy Name) nedir?

2-)İlk Temas: Yakalanan konuşmadaki ilk mesaj (comment) nedir?

3-)Dosya Transferi: Ann karşı tarafa bir dosya göndermiş. Bu dosyanın adı nedir?

4-)Dosya Analizi (File Carving):

Dosyayı trafikten dışarı aktarın (Export).

Dosyanın Magic Bytes (İlk 4 Hex karakteri) değeri nedir?

Dosyanın MD5 Hash değerini hesaplayıp yazın.

5-)Büyük İfşa: Mesajlarda veya dosyanın içinde geçen "Gizli Tarif" (Secret Recipe) tam olarak nedir? (İçeriği yazın).

1-)Suç Ortağı: Cool FileXfer (veya mesajlardaki isim).

2-)İlk Mesaj: "Here is the recipe!" (TCP Stream'in en üstünde Ann'in yazdığı ilk cümle).

3-)Dosya Adı: recipe.docx

4-)Magic Bytes: 50 4B 03 04

5-)

MD5 Hash Değeri: 5db54738737657b0a1864ed91dccf503

Büyük İfşa (Gizli Tarif): Dosyanın içinde sızdırılan bilgi: "1 cup of sugar, 2 cups of flour"

Göreviniz: evidence02.pcap dosyasını analiz ederek kaçış rotasını çizin:

1-)Kimlik Bilgileri: Ann'in kullandığı E-posta adresi nedir?

2-)Güvenlik İhlali: Ann e-postasına giriş yaparken hangi Şifreyi (Password) kullandı?

Not: SMTP trafiği şifrelenmemişse, parolayı açık metin (Cleartext) olarak görebilirsiniz.

3-)Gizli Sevgili: Ann'in e-posta attığı sevgilisinin (Mr. X) E-posta adresi nedir?

4-)Bavul Hazırlığı: Ann, sevgilisinden getirmesini istediği iki eşya (fake passport vb.) nedir?

Eklenti Analizi: Ann e-postaya bir dosya eklemiş.

5-)Bu eklentinin (Attachment) adı nedir?

Dosyayı dışarı aktarın ve MD5 Hash değerini yazın.

6-)Konum Tespiti: Eklentinin içindeki bilgileri (veya gömülü görselleri) inceleyerek; Ann ve sevgilisinin buluşacağı Şehir ve Ülke neresidir?

📋 Vaka Analiz Raporu: Ann'in Kaçış Planı

1-)Ann'in E-posta Adresi: sneakyg33k@aol.com

2-)Giriş Şifresi: 558r00lz

3-)Gizli Sevgili (Mr. X): mistersecretx@aol.com

4-)Bavul Hazırlığı (İki Eşya): Fake Passport (Sahte Pasaport) ve Bathing Suit (Mayo).

5-)Eklenti Adı: secretrendezvous.docx

Eklenti MD5 Hash: 6a8680cf5412226b524f55ae756745a9

6-)Buluşma Noktası:

Şehir: Playa del Carmen

Ülke: Meksika (Mexico)

BÖLÜM D: Mühendislik Vizyonu ve Etik (Reflection)

1. Kırmızı Çizgi: Etik ve Hukuk (TCK Kapsamı) Senaryo: Bir kafede oturuyorsunuz, Wireshark'ı açtınız ve ortak ağdaki (Public Wi-Fi) trafiği dinlemeye başladınız. Amacınız kötü olmasa bile, sadece merak etseniz bile;

Hukuki Boyut: Bu eylem, Türk Ceza Kanunu (TCK) kapsamında hangi suçlara girer? Özellikle Madde 243 (Bilişim Sistemine Girme) ve Madde 132 (Haberleşmenin Gizliliğini İhlal) bağlamında değerlendirin.

Halka açık ağlarda izinsiz paket dinlemek, TCK 243 uyarınca bilişim sistemine hukuka aykırı girmek ve TCK 132 uyarınca haberleşmenin gizliliğini ihlal etmek suçlarını oluşturur. Bu eylem, niyetin kötü olmasa bile haberleşme mahremiyetine dokunduğun için hapis cezasıyla sonuçlanabilecek ciddi bir suçtur. Kısacası; yazılı izin yoksa, yakaladığın her paket seni hukuki bir uçuruma sürükler.

Profesyonel Duruş: Bir Siber Güvenlik Uzmanı, yetkisi (yazılı izni) olmayan bir ağda neden asla "Promiscuous Mode" açmaz? Bu durum kariyerinizi nasıl bitirebilir?

Yazılı izin olmadan paket dinlemek kariyerine dijital format atmaktır; çünkü etik dışı bu hareket hem hapis cezası almana hem de sektördeki tüm güvenilirliğini bir anda kaybetmene neden olur.

2. Veri Yorumlama: "Görünenin Ötesi"

Soru: İşletim sistemleri (Windows/Linux) dosya türünü anlamak için genellikle uzantıya (.txt, .jpg) bakar. Ancak bir Adli Bilişimci (siz), dosyanın gerçek kimliğini anlamak için Magic Bytes (Hex Signature) verisine bakar.

Analiz: "Dosya uzantısına güvenme, içeriğe (Header) güven" prensibini teknik olarak açıklayın. Bir saldırgan dosya uzantısını değiştirse bile, neden dosyanın başındaki o sihirli baytları (Örn: PK.. veya MZ) değiştiremez? Değiştirirse dosya çalışır mı?

Çünkü dosya uzantıları kolayca değiştirilip gizlenebilir, ancak dosyanın "DNA'sı" olan Magic Bytes yalan söylemez. Eğer birisi bu baytları kafasına göre değiştirirse, ilgili program dosyayı tanıyamaz ve dosya asla çalışmaz, bozuk hatası verir.

3. Gürültü ve Sessizlik: "Ağda İz Bırakmak"

Basit bir Port Taraması (Nmap) bile ağda binlerce paket (gürültü) oluşturur.

Bu "gürültü", savunma tarafı (Blue Team / SOC) için neden bir avantajdır?

Saldırgan ne kadar çok paket gönderirse, arkasında o kadar çok ayak izi bırakır. Bu durum Blue Team için şu avantajları sağlar: Anomali Tespiti, Saldırganın İmzası (Kullandığı cihaz , saldırıda kullandığı ağın IP adresi...) ,Savunma Süresi Kazanma

Yorum: "Mükemmel suç yoktur, sadece incelenmemiş log (veya pcap) vardır" sözünü bu haftaki deneyiminizle yorumlayın.

Bu sözü bu hafta yaptığımız analizlerle bağdaştırırsak, aslında dijital dünyada hiçbir eylemi herhangi bir ipucu veya iz bırakmadan yapamayacağımızı görmüş olduk.