Bölüm A: Teori ve İstihbarat (Research & Logic)

1. Mekanik ve Altyapı:

- 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?

Ağ segmentinden geçen tüm frame'leri görebilmek için aktif edilir. Eğer bu mod kapalı olsaydı

-Multicast gruplara ait paketler,

- Broadcast paketler,

- Unicast paketleri kabul ederdi.

- 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?

Switch bulunan bir ağda sadece dinleme moduna geçmek yeterli değildir. Başka kullanıcıların trafiğini görebilmek için ya ARP tablosunu manipüle ederek trafiği kendi cihazı üzerinden geçirmek gerekir ya da switch üzerinde port mirroring yapılandırılması yapılmalıdır.

- 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?

Firewall log kaydı, trafiğin özetini gösterir; pcap dosyası ise trafiğin ham halini içerir. Çoğunlukla bir olay müdahalesinde kesin delil olarak pcap kabul edilir. Çünkü ham veriyi içerdiği için sonradan tekrar incelenebilir ve teknik olarak doğrulanabilir. Log kayıtları ise daha çok destekleyici niteliktedir.

2. Protokol Anatomisi:

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

“İşlem yapmak istiyorum” (SYN) -> “Hazırım” (SYN-ACK) -> " Başlayalım” (ACK).

- TCP vs. UDP: Neden YouTube veya Netflix yayını izlerken (Streaming) genellikle UDP, banka hesabımıza girerken TCP tercih edilir? "Hız" ve "Güvenilirlik" kavramları üzerinden açıklayın.

Streaming’de hız önceliklidir. UDP paket kaybı olursa tekrar göndermez ve veri akışı devam eder, bu yüzden yayın takılmaz bozulmalar olabilir. Banka işlemlerinde ise güvenilirlik önceliklidir. TCP paket kaybı olursa yeniden gönderir ve verinin eksiksiz ulaşmasını sağlar. Bu biraz daha yavaş olabilir ama veri bütünlüğü korunur.

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

Paketlerin üzerine numara yazılmasının amacı, verinin doğru sırayla birleştirilmesini sağlamaktır. Farklı yollardan giden paketler olabileceği için hedefe yanlış sırayla gidebilir.

Eğer 5. paket, 3. paketten önce gelirse bilgisayar sıra numarasına bakarak eksik olan paketi bekler. Gerekirse göndericiden tekrar ister ve veriyi doğru sıraya koyarak üst katmana iletir.

3. Kimlik ve Adresleme:

- 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?

ARP, yerel ağda broadcast gönderir: “192.168.1.1 kimde?” şeklinde tüm cihazlara sorar. Bu IP’ye sahip olan cihaz kendi MAC adresini cevap olarak gönderir. Böylece gönderen bilgisayar, IP ile MAC eşleşmesini öğrenir ve veriyi doğru fiziksel adrese iletir.

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

önce ağda bir DHCP sunucusu var mı diye Discover mesajı yayınlar. DHCP sunucusu uygun bir IP adresi önererek Offer gönderir. Bilgisayar bu teklifi kabul ettiğini belirtmek

için Request mesajı yollar. Son olarak sunucu Acknowledge göndererek IP adresini resmen atar ve bağlantı aktif hale gelir.

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

Tarayıcıya google.com yazdığımızda önce bu ismin IP karşılığı kontrol edilir. Eğer yerel önbellekte yoksa, tanımlı olan DNS sunucusuna bir DNS sorgusu (query) gönderilir. DNS sunucusu bu alan adının IP adresini bulur ve DNS cevabı (response) olarak geri gönderir. Bilgisayar da aldığı IP adresi üzerinden ilgili sunucuya bağlantı kurar ve siteyi açar.

4. Şifreleme ve Kör Noktalar:

- 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?

HTTPS trafiği TLS ile şifrelendiği için Wireshark ile paketi yakalasak bile kullanıcı adı ve şifreyi doğrudan göremeyiz. Ancak bir analist kaynak ve hedef IP adresleri, kullanılan port (genellikle 443), bağlantı zamanı, sertifika bilgileri SNI (Server Name Indication) gibi meta verileri görebilir.

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

Sahte sertifika sunmasının amacı, kurbanı gerçek sunucu yerine kendisine güvenmeye ikna etmektir. Böylece istemci ile saldırgan arasında bir TLS bağlantısı, saldırgan ile gerçek sunucu arasında ayrı bir TLS bağlantısı kurulur.

5. Saldırı İmzaları:

- 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?

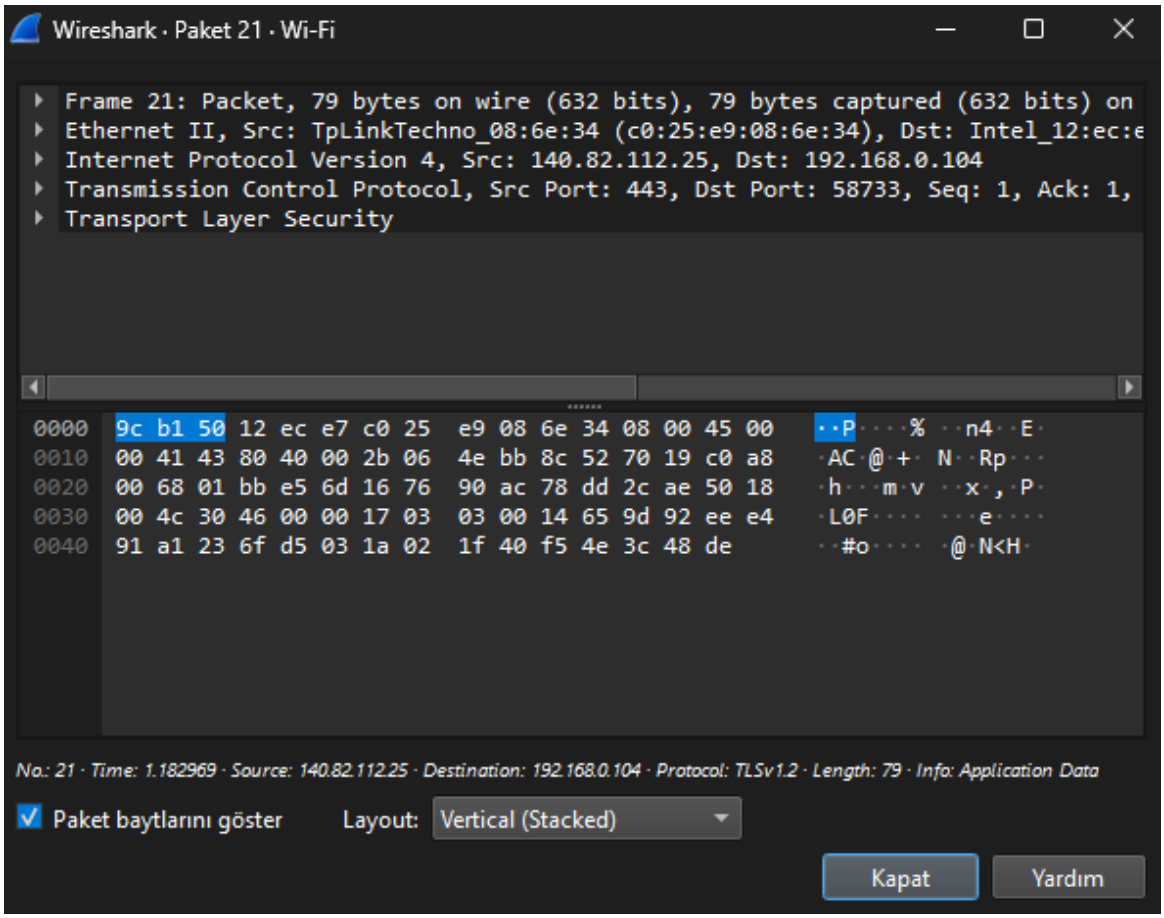
Normal bir bağlantıda SYN → SYN-ACK → ACK ile süreç tamamlanır. Port taramasında ise birçok porta art arda SYN gönderilir, ancak genellikle bağlantı tamamlanmaz. Wireshark'ta bu durum, farklı portlara giden çok sayıda SYN paketi ve yarım kalan bağlantılar şeklinde görülür.

- Denial of Service (DoS): Bir sunucuya saniyede 100.000 adet SYN paketi gelmesi (SYN Flood) sistemi nasıl kilitler?

SYN Flood saldırısında sunucuya çok sayıda SYN paketi gönderilir. Sunucu her biri için bağlantı başlatır ve ACK bekler, ancak saldırgan son adımı tamamlamaz. Bu yüzden yarım açık bağlantılar birikir, bağlantı kuyruğu dolar ve gerçek kullanıcılar sisteme bağlanamaz. Böylece sistem kilitlenmiş olur.

Bölüm B: Saha Eğitimi ve Araç Hakimiyeti

1. Arayüz ve Renkler
- "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 21

- 79 byte uzunluğunda
- Hem kablo üzerinde hem capture sırasında 79 byte olarak alınmış

Ethernet II (Layer 2)

Bu bölüm fiziksel ağ seviyesini temsil eder. Paket hangi cihazdan çıkmış ve yerel ağda hangi cihaza yönelmiş onu gösterir.

Internet Protocol Version 4 (Layer 3)

Bu katman, paketin internet seviyesinde hangi IP'den hangi IP'ye gittiğini gösterir. 140.82.112.25 büyük ihtimalle dış bir sunucu, 192.168.0.104 ise yerel ağdaki cihaz.

Transmission Control Protocol (Layer 4)

Bu bölüm TCP bağlantı detaylarını içerir. 443 portu olduğu için trafik HTTPS üzerinden geliyor.

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

Pakette kırmızı veya siyah arka plan, olağan dışı bir durum olduğunu gösterir. Bu renkler analistin o paketi özellikle incelemesi gerektiğini gösterir.

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

Yazmamız gereken Wireshark display filter komutu:

```
ip.addr == 10.10.10.10 and tcp.port == 80
```

- Bu filtreyi uyguladığınızda (TryHackMe'deki örnek pcap üzerinde veya kendi trafiğinizde) filtre çubuğunun yeşil yandığı anın ekran görüntüsü.

3. OSI ile Paket İlişkisi
- Packet Details panelinde Ethernet II başlığını genişletin. Burada gördüğünüz "Source" ve "Destination" adresleri, OSI modelinin hangi katmanına (Layer) aittir?

Ethernet II başlığı altında görülen Source ve Destination adresleri OSI modelinde Layer 2 (Data Link Layer) katmanına aittir.

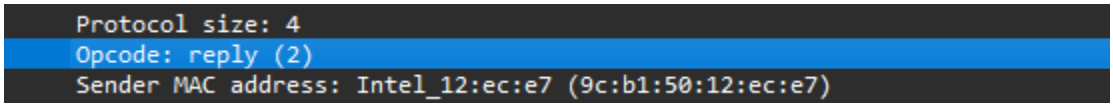
4. ARP Trafiği

- 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 anlamına gelir. Yani “Bu IP kimde?” şeklinde yapılan sorgudur.

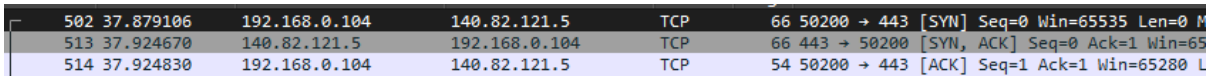
Opcode 2: ARP Reply anlamına gelir. IP adresine sahip olan cihazın, kendi MAC adresini bildirdiği cevaptır.

- Kanıt: Pcap dosyasındaki bir ARP paketinin "Opcode" satırını genişleterek ekran görüntüsü alın.



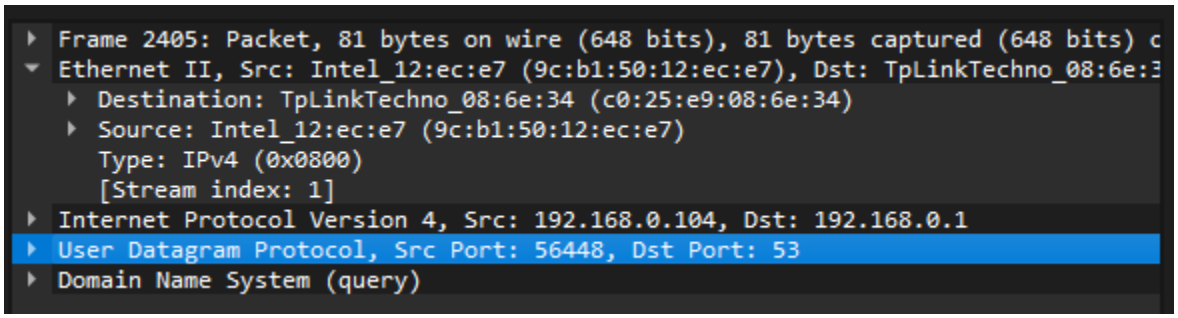
5. TCP El Sıkışması

- Görev: Trafik içinde 3-Way Handshake (SYN -> SYN/ACK -> ACK) işlemini bulun. Kanıt: Bu üç paketi alt alta (veya filtreleyerek) gösteren ekran görüntüsü. Sequence Number değerlerinin nasıl arttığına dikkat edin.



6. DNS Sorguları

- Soru: Bir bilgisayar google.com'a gitmek istediğinde önce DNS sunucusuna sorar. Sorgu paketi (Query) hangi protokolle gider? (TCP/UDP?) Kanıt: Standard query başlığını içeren bir DNS paketinin detay görüntüsü.



User Datagram Protocol: UDP

7. Saldırı Analizi

- Soru: Bu görevde saldırgan, sisteme sızmak için bir "Exploit" kullanıyor. Wireshark bu tür şüpheli durumları genellikle kırmızı ile işaretler veya uyarı verir. Kanıt: Saldırıyı ele veren o kritik paketin veya akışın ekran görüntüsü.

Bölüm C: Vaka Analizi

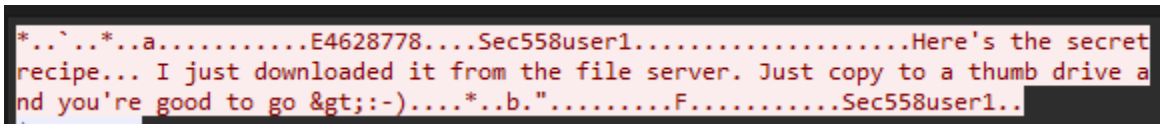
Vaka 1: Köstebek Avı (Ann's Bad AIM)

Senaryo: Şirket çalışanlarından Ann Dercover'ın, rakip firmaya "Gizli Tarif"i (Secret Recipe) sızdırdığından şüpheleniyoruz. Güvenlik ekibi, Ann'in bilgisayarından (192.168.1.158) çıkan şüpheli bir "Anlık Mesajlaşma" (IM - AIM Protocol) trafiği yakaladı.

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

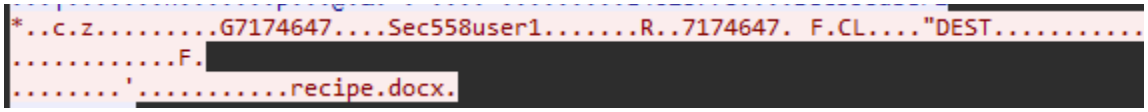
Sec558user1

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



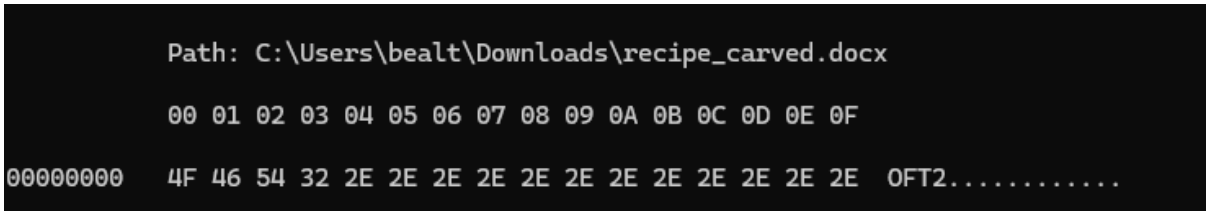
Here’s the secret recipe…

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

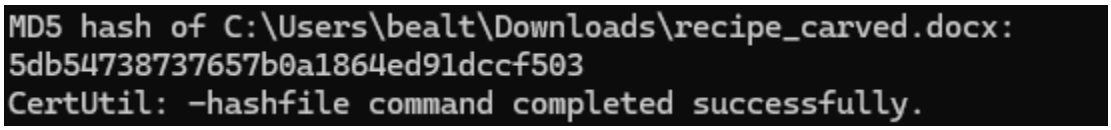


Recipe.docx

- Dosya Analizi (File Carving): Dosyayı trafikten dışarı aktarın (Export). Dosyanın Magic Bytes (İlk 4 Hex karakteri) değeri nedir? Dosyanın MD5 Hash değerini hesaplayıp yazın.



4F 46 54 32



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

Vaka 2: Kaçış Planı

Senaryo: Vaka 1'deki olaydan sonra Ann kefaletle serbest bırakıldı ancak ortadan kayboldu! Polis, Ann'in kaçmadan hemen önce "Gizli Sevgilisi" (Mr. X) ile E-posta (SMTP) yoluyla iletişime geçtiğini düşünüyor. Kaçtığı yeri bulmamız lazım.

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

```
MAIL FROM: <sneakyg33k@aol.com>
```

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

```
AUTH LOGIN

334 VXNlcm5hbWU6

c25lYWt5ZzMza0Bhb2wuY29t

334 UGFzc3dvcmQ6

NTU4cjAwbHo=

235 AUTHENTICATION SUCCESSFUL
```

NTU4cjAwbHo=

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

```
RCPT TO: <sec558@gmail.com>
```

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

```
Hi sweetheart! Bring your fake passport and a bathing suit. Address =
attached. love, Ann
------=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/html;
          charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

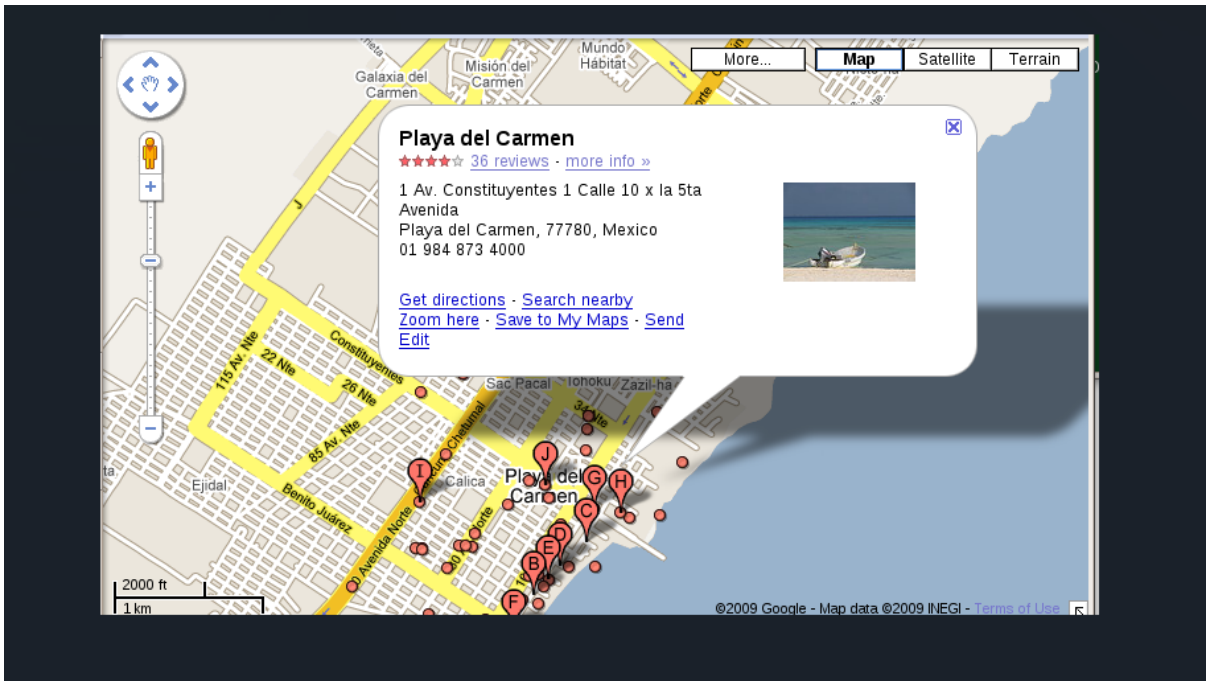
sahte pasaport ve mayo

- Eklenti Analizi: Ann e-postaya bir dosya eklemiş. Bu eklentinin (Attachment) adı nedir? Dosyayı dışarı aktarın ve MD5 Hash değerini yazın

```
------=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: application/octet-stream;
          name="secretrendezvous.docx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
          filename="secretrendezvous.docx"
```

```
Algorithm       Hash
---------       ----
MD5             9E423E11DB88F01BBFF81172839E1923
```

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



Playa del Carmen, 77780, Mexico

Bölüm D: Mühendislik Vizyonu ve Etik

1. Kırmızı Çizgi: Etik ve Hukuk

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.

Ağ üzerinde başka cihazların sistemlerine (örneğin açık portlara, paylaşıma, router arayüzüne) yetkisiz erişmeye çalışırsan,

Paket manipülasyonu (ARP spoofing, MITM vb.) yaparsan,

Bu durumda 243 devreye girer.

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

Bir siber güvenlik uzmanı, yetkisi olmayan bir ağda promiscuous mode açmaz çünkü bu, başkalarının ağ trafiğini izlemek anlamına gelir ve hukuken suç sayılabilir. Türk Ceza Kanunu kapsamında haberleşmenin gizliliğini ihlal eder.

2. Veri Yorumlama: "Görünenin Ötesi"
- "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?

Dosya uzantısı sadece isimdir ve kolayca değiştirilebilir. Gerçek dosya türünü belirleyen şey dosyanın başındaki magic bytes (header) bilgisidir. İşletim sistemi dosyayı açarken bu imzaya göre yapıyı okur. Saldırgan uzantıyı değiştirebilir ama header'ı değiştirirse dosyanın yapısı bozulur ve büyük ihtimalle çalışmaz. Bu yüzden uzantıya değil, içeriğe güvenilir.

3. Gürültü ve Sessizlik:
- Bir saldırganın "Sessizce sızdım" demesi teknik olarak ne kadar mümkündür?

Saldırgan tespit edilmemiş olabilir ama sistemlerde mutlaka log oluşur. Ne kadar sessizce sızdım dese de mutlaka bir iz bırakmıştır ve takip edilebilir.

- Basit bir Port Taraması (Nmap) bile ağda binlerce paket (gürültü) oluşturur. Bu "gürültü", savunma tarafı (Blue Team / SOC) için neden bir avantajdır?

Port taraması çok sayıda istek paketi üretir ve bu normal kullanıcı trafiğine benzemez. Bu anormal yoğunluk, savunma sistemleri (IDS/IPS, SIEM) için kolayca fark edilir bir davranıştır. Yani saldırgan için "gürültü" olan şey, Blue Team için erken uyarı sinyalidir.

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

Suçu ne kadar mükemmel işlediği düşünülse de yaptığı etkiler iz bırakır. Odağı başka yere çevirmek bile yeterli değildir. Bir tane iz bile her şeyi ele verebilir.