Bölüm A: Teori ve İstihbarat (Research & Logic)

1. Mekanik ve Altyapı: "Ağı Dinlemek"

Promiscuous Mode

Wireshark'ı açtığımızda promiscuous mode'u aktif ediyoruz çünkü normalde ağ kartımız sadece kendine gelen paketleri dinler. Bu mod kapalı olsaydı, sadece bizim bilgisayara adreslenmiş paketleri görebilirdik - yani broadcast'lar ve bizim IP/MAC adresimize giden trafik. Ağdaki diğer cihazlar arasındaki konuşmaları hiç göremezdik.

Hub vs. Switch

Hub kullandığımızda zaten sorun yoktu, çünkü hub elektrik prizesi gibi çalışır - gelen her şeyi herkese dağıtır. Ama switch akıllı, trafiği sadece hedef cihaza gönderir. Switch ortamında A' nın B' ye gönderdiği paketi görmek için ya ARP Poisoning yapıp "ben B'yim" diye switch'i kandırırız, ya da ağ yöneticisiyseniz port mirroring (SPAN) özelliğini kullanıp belirli bir portun trafiğini kendi portunuza kopyalatırsınız.

Pcap vs. Log

Firewall logu özet rapor gibidir: "10:30'da Fatma , Google'a bağlandı" der, o kadar. Pcap ise gerçek paketin kendisi - sanki ses kaydı gibi. Olay müdahalesinde pcap kesin delildir çünkü içinde paketin bütün detayları var: kim ne göndermiş, hangi bayraklar set edilmiş, payload ne... Log'da birisi "blocked" yazmış olabilir ama pcap'te gerçekte ne olduğunu görürsünüz.

2. Protokol Anatomisi: "Dijital El Sıkışma"

3-Way Handshake

Telefon görüşmesine benzetebiliriz: Sen telefonu açıp "Alo?" dersin (SYN), karşı taraf "Alo, buyurun" der (SYN-ACK), sen de "Tamam konuşabiliriz" dersin (ACK). İşte o zaman görüşme başlar. TCP de aynen böyle - önce iki taraf da hazır olduğundan emin olmalı.

TCP vs. UDP

Film izlerken birkaç piksel kaybetsen fark etmezsin, önemli olan akışın durmaması - bu yüzden UDP. Paket kaybolunca "neyse" der, devam eder. Ama banka hesabına girerken her rakamın doğru gitmesi lazım, TCP kullanılır. Paket kaybolursa TCP "dur, o paketi tekrar gönder" der, her şey tamamlanana kadar bekler. UDP hızlı ama dikkatsiz, TCP yavaş ama güvenilir.

Sequence Number

Paketleri numaralandırıyoruz çünkü internet kargolar gibi - bazen 3. paket 1.'den önce gelir. Bilgisayar numaralara bakıp "tamam, 2 geldi, 1 geldi, 3 geldi" diye sıraya koyar. 5 gelip de 3 yoksa, bekler veya 3'ü tekrar ister. Böylece "Merhaba" yerine "bahMera" gibi karışık şeyler almayız.

3. Kimlik ve Adresleme: "Postacı Kapıyı Çalar"

ARP Protokolü

IP adresini biliyoruz ama ethernet seviyesinde MAC adresi lazım. Bilgisayar bağırır gibi broadcast yapar: "192.168.1.1'in MAC adresi kimde?" Ağdaki herkes duyar ama sadece o IP'ye sahip olan "bende, işte MAC'im: AA:BB:CC..." diye cevap verir. Artık direkt MAC adresine gönderebilirsin.

DHCP (DORA)

Yeni bir laptop ağa takıldı, IP'si yok. Önce "Kimse bana IP verir mi?" diye sorar (Discover), DHCP sunucusu "Al sana 192.168.1.50" der (Offer), laptop "tamam alıyorum" der (Request), sunucu da "onaylandı, 24 saat senin" der (Acknowledge). Böylece IP sahibi olur.

DNS

google.com yazınca bilgisayar "bu ismin IP'si ne?" diye DNS sunucusuna sorar. DNS sunucusu kendi biliyorsa cevaplar, bilmiyorsa başka DNS'lere sorar, sonunda bir IP döndürür. Artık bilgisayar bu IP'ye bağlanır. DNS internet için telefon rehberi gibidir.

4. Şifreleme ve Kör Noktalar: "Sır Perdesi"

HTTPS ve Şifreleme

HTTPS paketini yakaladığımızda içini okuyamayız - sanki mühürlü zarf görmüşüz gibi. Kullanıcı adı şifre göremeyiz. Ama meta-data kalır: kim kiminle konuşmuş (IP), hangi site (SNI: Server Name Indication), ne zaman, ne kadar veri - bunları görürüz. İçerik şifreli ama "kim kimle ne zaman konuştu" bilgisi açık.

Man-in-the-Middle

Şifreli trafiği çözmek için araya girip sahte sertifika sunarsın. Kullanıcıya "ben Google'ım" dersin, kullanıcı sana şifreli bağlanır, sen de gerçek Google'a bağlanırsın. Ortada olduğun için şifreyi çözüp okuyup tekrar şifrelersin. Ama bu işe yaraması için kullanıcının sahte sertifikayı kabul etmesi lazım.

5. Saldırı İmzaları: "Suçluyu Tanımak"

Port Taraması

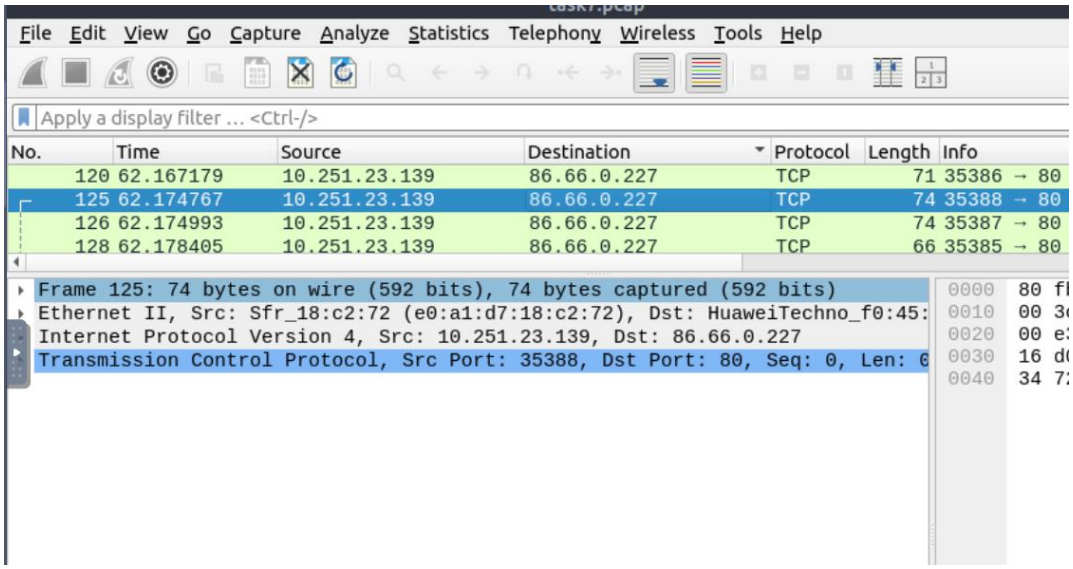
Normal bağlantı: SYN gönderirsin, SYN-ACK gelir, ACK gönderirsin, konuşursun, bağlantıyı düzgün kapatırsın. Port taraması: binlerce porta SYN gönderirsin, açık olanlar SYN-ACK döner, ama sen ACK göndermezsin, direkt RST atıp kapatırsın. Wireshark'ta "bir sürü SYN, hiç tamamlanmamış bağlantı" görürsün.

Denial of Service (DoS)

Sunucu her SYN paketi aldığında "tamam biri bağlanacak" diye hafızada yer ayırır, SYN-ACK gönderip ACK bekler. Ama saldırgan 100.000 SYN gönderip hiç ACK göndermiyor. Sunucunun hafızası yarım kalmış bağlantılarla doluyor, yeni meşru kullanıcılara yer kalmıyor. Sistem "bekle bekle bekle" derken kilitlenir.

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

1-



Frame: Wireshark'ın yakaladığı ham paketin tamamı - byte sayısı, yakalanma zamanı gibi fiziksel bilgiler burada.

Ethernet II: Yerel ağdaki kaynak ve hedef MAC adreslerini içeren katman - paket switch/router'da hangi porta gidecek bunu belirler.

Internet Protocol (IP): Kaynak ve hedef IP adreslerinin olduğu katman - paketin internette nereden nereye gideceğini belirler.

Transmission Control Protocol (TCP): Port numaraları, sequence number, bayraklar (SYN, ACK) gibi bilgilerin olduğu katman - güvenilir veri iletimi için kullanılır.

Kırmızı paketler genellikle ağ sorunlarını gösterir - paket kaybolmuş, tekrar gönderilmiş, bağlantı kopmuş gibi. Analist olarak bunları görünce "ağda performans sorunu mu var, yoksa saldırı mı?" diye bakmaya başlarsın.

Siyah paketler daha ciddi - paket tamamen bozulmuş veya protokol kurallarına uymamış demektir.

Kısacası, bu renkler uyarı lambası gibidir. Normal yeşil/mavi paketler arasında kırmızı görünce "dur bakalım, burada ne olmuş?" diye dikkat kesilirsin. Özellikle çok sayıda kırmızı paket varsa, ya ağda fiziksel sorun var ya da birisi kötü niyetli bir şeyler yapıyor olabilir.

Kırmızı paket:

- Açabilirsin, okuyabilirsin
- Ama "neden tekrar geldi?" diye sorarsın
- **Ağ performansı** sorunlu

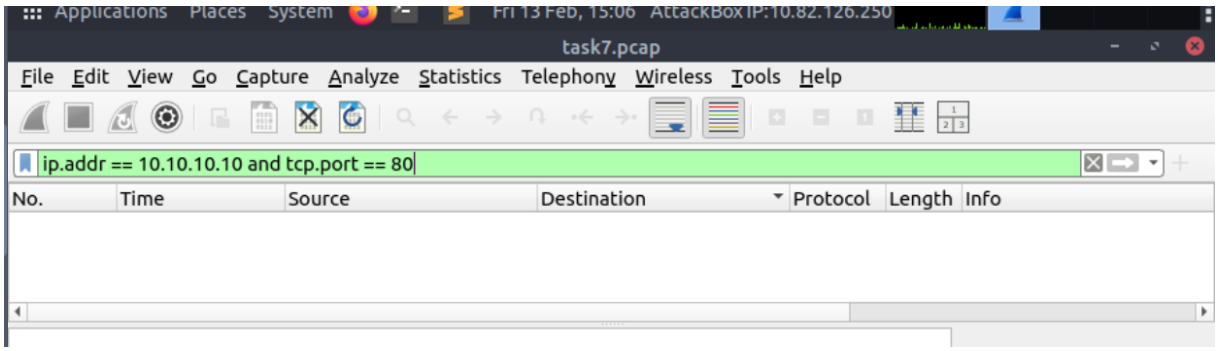
Siyah paket:

- Açamayabilirsin bile
- İçi bozuk/anlamsız

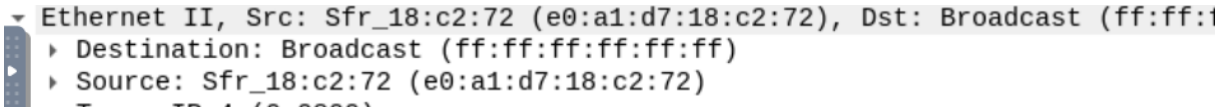
- **Donanım/kablo** sorunlu olabilir

- **Kırmızı:** "Trafik akışında sorun var"
- **Siyah:** "Paketin kendisi bozuk"

2



3



MAC adresleri - OSI modelinin **2. katmanı** (Data Link Layer)

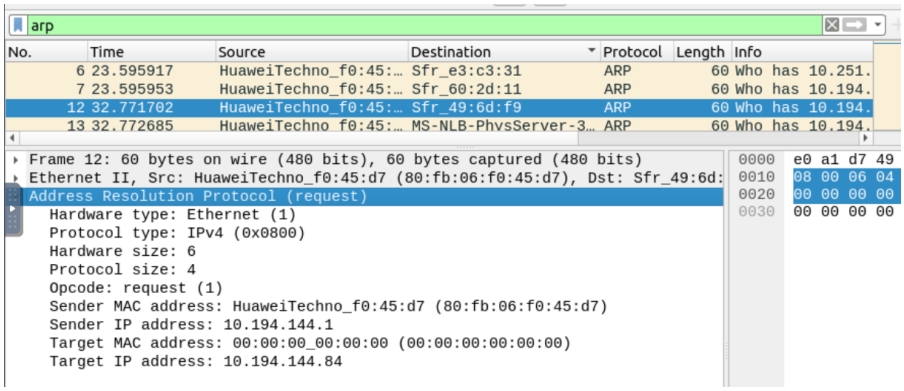
4

Opcode 1 = ARP Request (İstek)

- "Bu IP adresinin MAC adresi nedir?" sorusu
- Broadcast olarak ağdaki herkese gönderilir

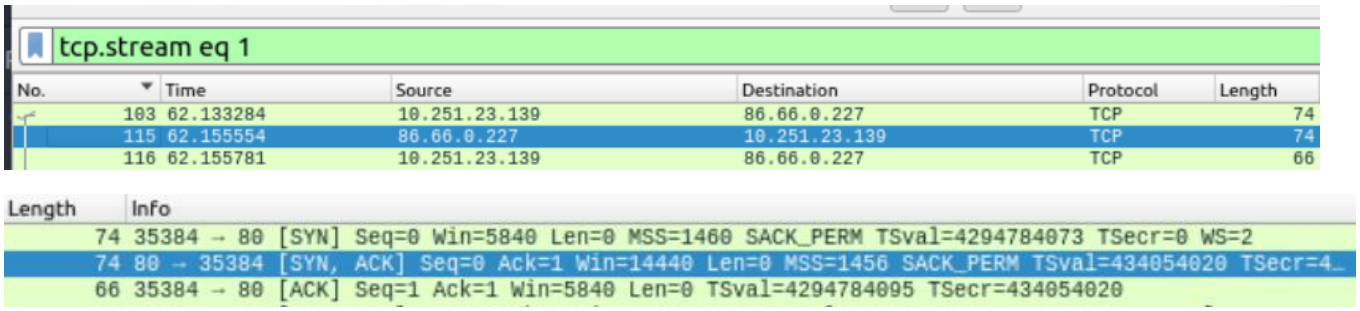
Opcode 2 = ARP Reply (Cevap)

- "Benim MAC adresim bu" cevabı
- Sadece soruyu sorana gönderilir



Opcode:1 request

5



Paket 103: [SYN] - İstemci bağlantı isteği gönderiyor **Paket 115:** [SYN, ACK] - Sunucu "tamam" diyor
Paket 116: [ACK] - İstemci onaylıyor

Info sütununda sequence number'lar görünüyor:

1. Paket (SYN):

Seq=0, Win=5840

2. Paket (SYN, ACK):

Seq=0, Ack=1, Win=14448

3. Paket (ACK):

Seq=1, Ack=1, Win=5840

Sequence Number Nasıl Artıyor?

İstemci tarafı:

- SYN: Seq=0
- ACK: Seq=1 (0+1=1) ✓

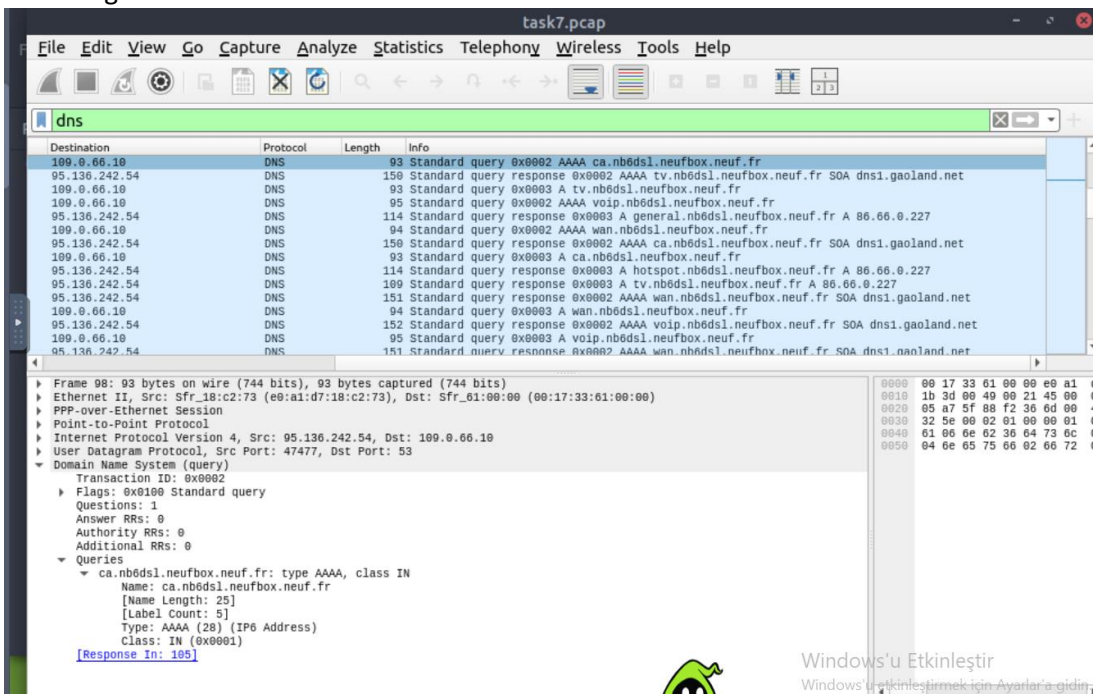
Sunucu tarafı:

- SYN,ACK: Seq=0, Ack=1 (istemcinin Seq'ini onaylıyor) ✓

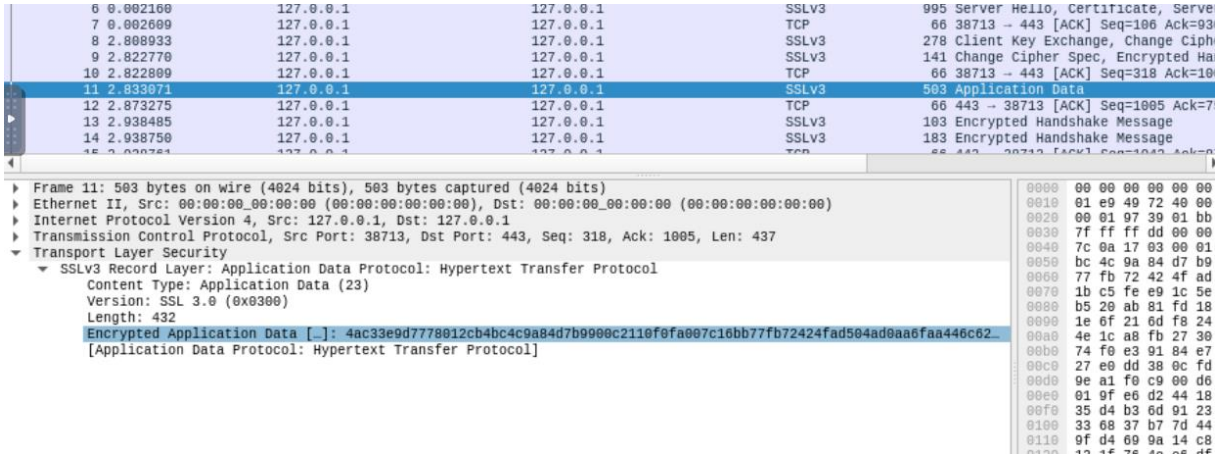
3 paket var (SYN → SYN,ACK → ACK)
Sequence number'lar artıyor (0 → 1)
Acknowledgment number'lar doğru (Ack=1)

6

UDP ile gider

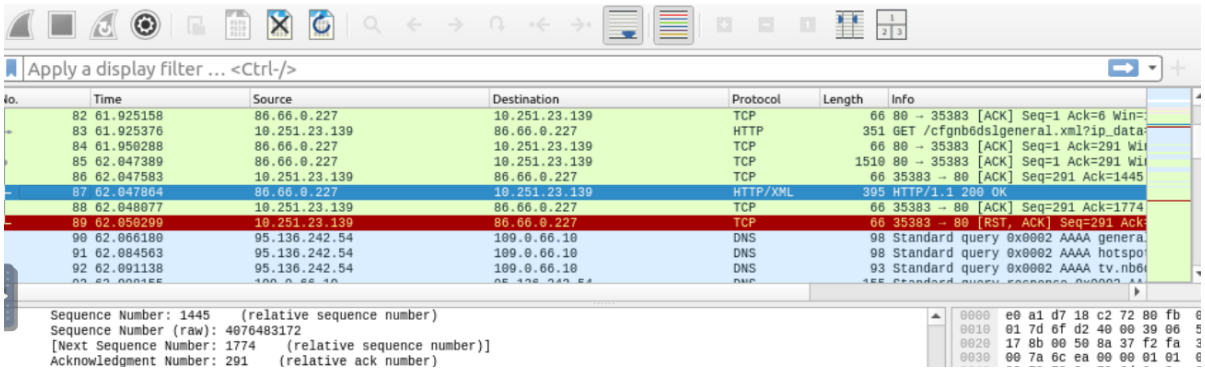


7



Şifreli gözüküyor

8

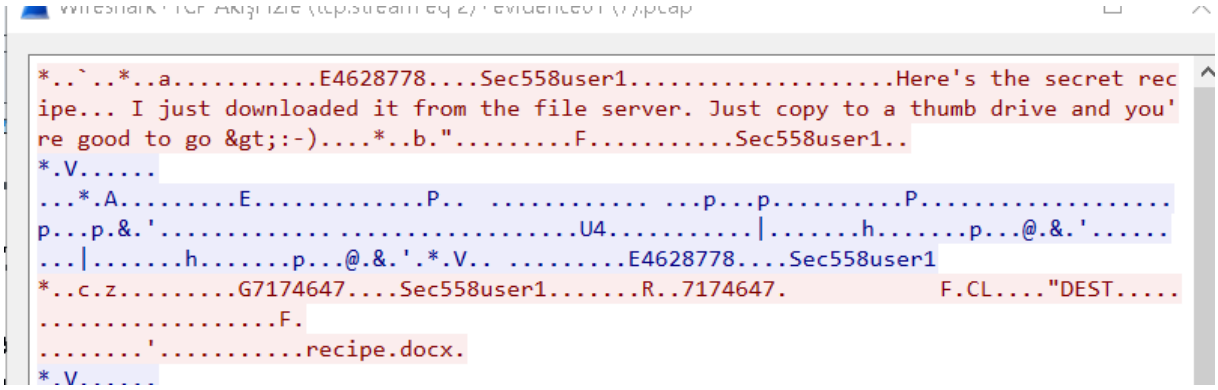


89 numaralı olan

BÖLÜM C: Vaka Analizi (Evidence Files)

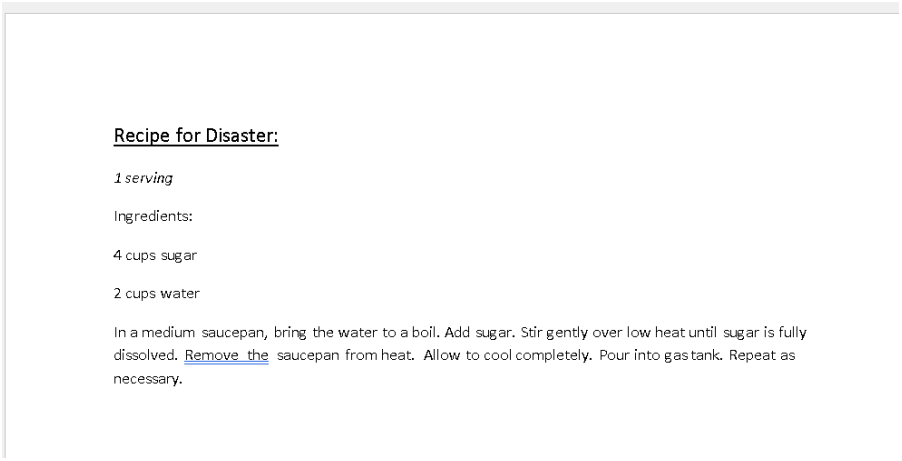
Vaka 1:

1- Sec558user1
2- Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-
3- recipe.docx
4- DOCX
50 4B 03 04
52c13d8c0a99ac0d3210e8e8edb046bf



5- İçerik

Uzantısını .docx yaptım.



Recipe for Disaster:

1 serving

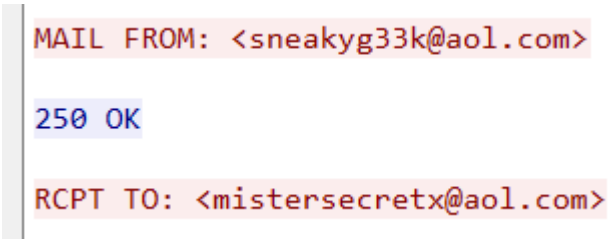
Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Vaka 2

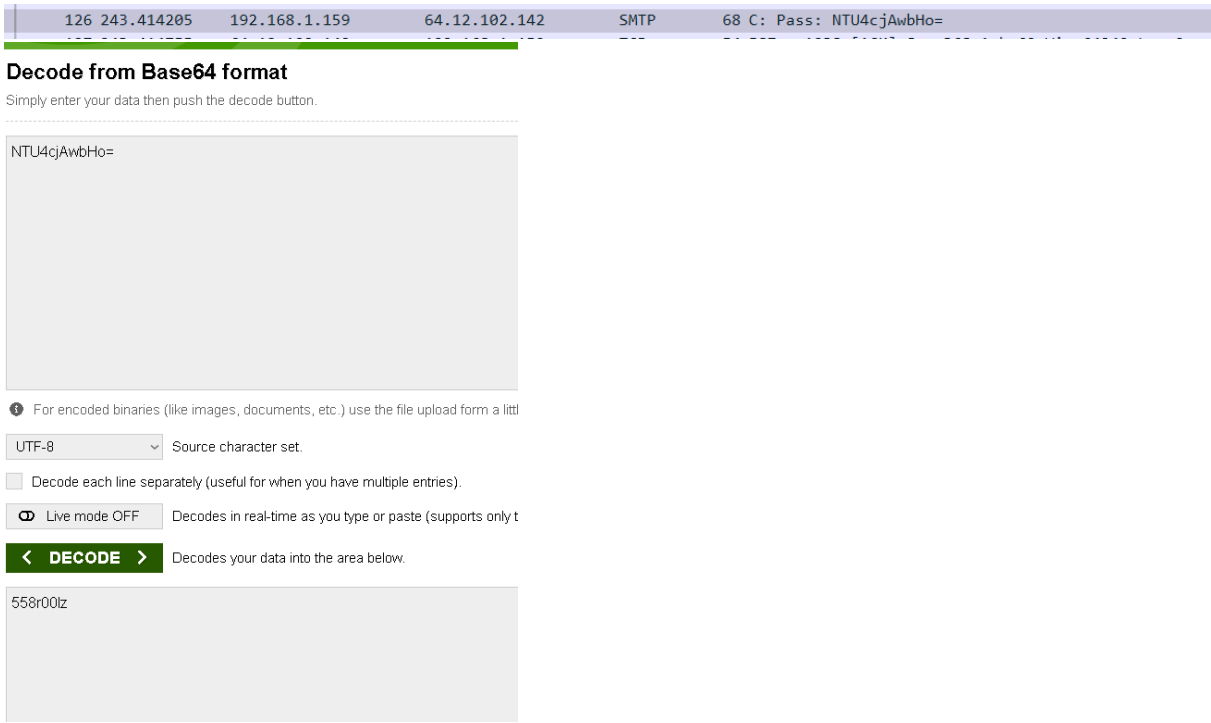


```
MAIL FROM: <sneakyg33k@aol.com>

250 OK

RCPT TO: <mistersecretx@aol.com>
```

1- sneakyg33k@aol.com

2- 

```
126 243.414205    192.168.1.159    64.12.102.142    SMTP    68 C: Pass: NTU4cjAwbHo=
```

Decode from Base64 format

Simply enter your data then push the decode button.

NTU4cjAwbHo=

For encoded binaries (like images, documents, etc.) use the file upload form a litt

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only t

DECODE Decodes your data into the area below.

558r00lz

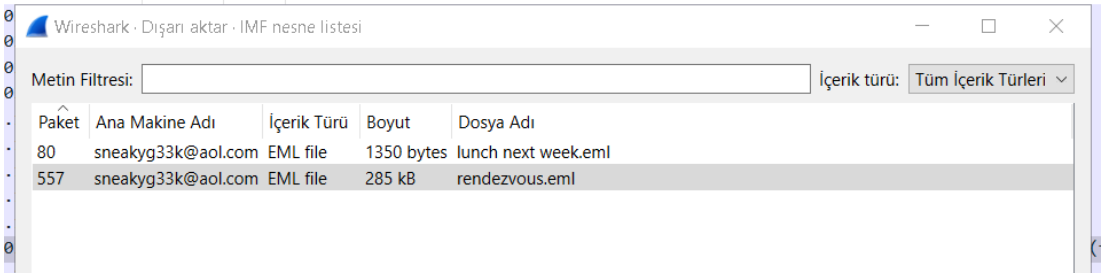
558r00lz

3- mistersecretx@aol.com

4-
```
Hi sweetheart! Bring your fake passport and a bathing suit. Address =
attached. love, Ann
```

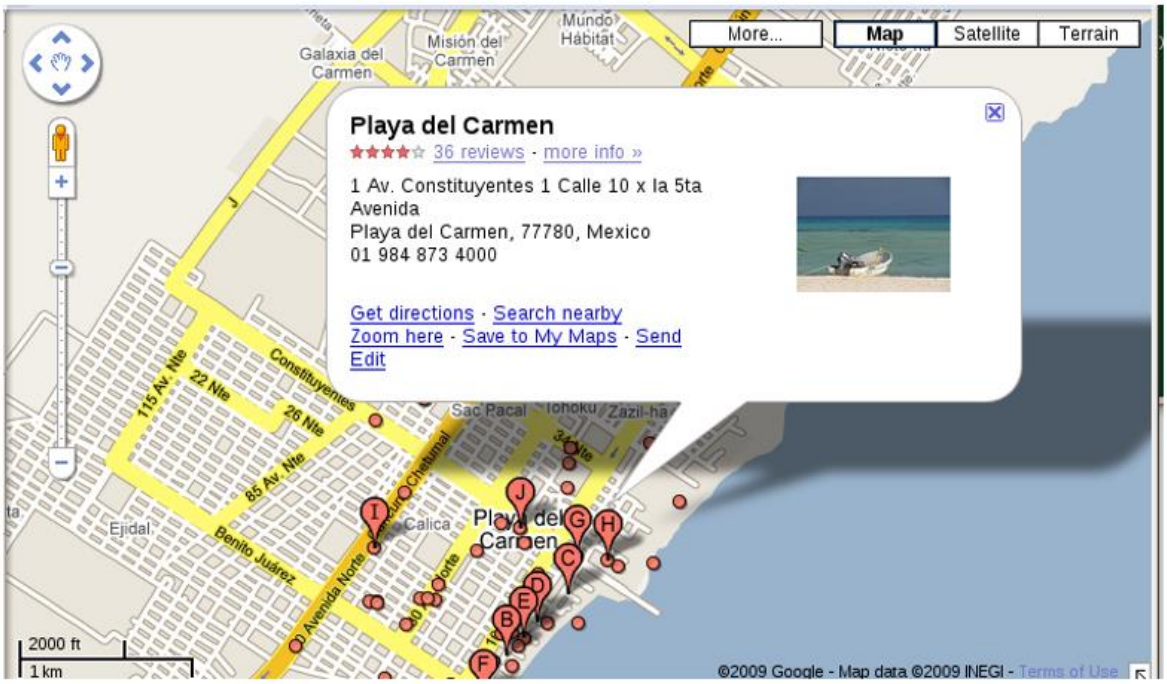
5- secretrendezvous.docx

9e423e11db88f01bbff81172839e1923



6-

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.



□ BÖLÜM D: Mühendislik Vizyonu ve Etik (Reflection)

Hukuki Boyut:

Kafede Wireshark açıp başkalarının trafiğini dinlemek **suçtur**, "meraktan" yaptım demeniz bir şeyi değiştirmez.

TCK Madde 243 (Bilişim Sistemine Girme): Başkalarının iletişimini izinsiz dinlemek, onların "bilişim sistemine" yetkisiz erişim anlamına gelir. Sisteme girmek için fiziksel erişim gerekmez - ağdaki trafiği yakalamak bile yeterli. Ceza: 1-3 yıl hapis.

TCK Madde 132 (Haberleşmenin Gizliliğini İhlal): İnsanlar kafede Instagram'a girdiğinde, mail attığında, haberleşme yapıyor. Siz bunu izinsiz dinliyorsunuz. Anayasa'nın 22. maddesi "haberleşme gizliliği"ni korur. Ceza: 1-3 yıl hapis.

Sonuç: "Ben bir şey yapmadım ki, sadece baktım" demek işe yaramaz. Mahkeme'de "merak ettim" diyerek kurtulmazsınız.

Profesyonel Duruş:

Bir siber güvenlik uzmanı olarak **yazılı izin** olmadan asla Promiscuous Mode açmazsınız çünkü:

1. **Kariyer sonu:** Yakalanırsanız, sektörde bir daha iş bulamazsınız. Kimse size güvenmez.
2. **Hukuki sorumluluk:** Şirketiniz sizi korumaz, siz tek başınıza mahkemelik olursunuz.
3. **Etik ihlal:** Sertifikalarınız (CEH, OSCP) iptal edilebilir.

Örnek: Bir penetrasyon testçisi, müşteri ağında bile önce "Rules of Engagement" (çalışma kuralları) imzalar. Hangi IP'lere bakabileceği, hangi saatlerde çalışacağı yazılıdır. Kafedeki Wi-Fi'da böyle bir izin yok!

Kısaca: Merak kötü niyetli olmayabilir ama hukuk bunu umursamaz. Yetkisiz dinleme = suç.

2. Veri Yorumlama: "Görünenin Ötesi"

İşletim sistemleri dosya türünü anlamak için uzantıya bakar: foto.jpg → "bu resim". Ama **saldırganlar bunu kandırır:**

virus.exe → virus.jpg olarak değiştir

Windows bunu "resim" sanır ama **gerçekte exe dosyasıdır.**

Adli bilişimci ne yapar?

Dosyanın **Magic Bytes** (ilk birkaç byte) değerine bakar:

JPEG: FF D8 FF E0

PNG: 89 50 4E 47

EXE: 4D 5A (MZ)

ZIP: 50 4B 03 04 (PK)

Uzantı virus.jpg bile olsa, ilk bytelar 4D 5A ise → **Bu bir EXE dosyası!**

Saldırgan Magic Bytes'ı Değiştiremez mi?

Teknik olarak değiştirebilir ama dosya çalışmaz:

Orijinal virus.exe:

4D 5A 90 00 ... (EXE header)

Saldırgan değiştirdi:

FF D8 FF E0 ... (JPEG header koydu)

Ne olur?

- Windows bunu çalıştırmaya kalkar → "Geçersiz dosya" hatası
- JPEG olarak açarsan → Bozuk resim, açılmaz

Neden?

Magic Bytes sadece "etiket" değil, **dosyanın yapısını tanımlayan bilgidir.** EXE dosyası, MZ header'ından sonra belirli bir yapı bekler (PE format). JPEG header koyarsanız, program "buradan sonra resim verisi gelecek" bekler ama virüs kodu gelir → çöker.

Sonuç: Uzantı değiştirmek kolay, Magic Bytes değiştirmek dosyayı bozar. Bu yüzden adli bilişimciler **içeriğe** güvenir.

3. Gürültü ve Sessizlik: "Ağda İz Bırakmak"

Saldırgan "Sessizce" Sızabilir mi?

Teknik olarak çok zor, neredeyse imkansız.

Basit bir **Nmap port taraması** bile:

nmap -p- 192.168.1.0/24

→ 65535 port × 254 IP = ~16 milyon paket!

Bu kadar paket gönderip "fark edilmedim" demek saçmalık.

Hatta en sessiz saldırılar bile iz bırakır:

- SSH ile girdiyseniz → Login logu var

- Dosya indirdiyseniz → Network trafiği var
- Komut çalıştırdıysanız → Bash history var

Blue Team İçin Avantaj:

Saldırgan ne kadar "gürültü" yaparsa, savunmanın işi o kadar kolay:

SOC Analisti:

"192.168.1.50'den 1 dakikada 10.000 SYN paketi!"

→ Port taraması! Alarm!

"user123 gece 03:00'te login olmuş"

→ Şüpheli! İncele!

SIEM, IDS, Firewall bu gürültüyü tespit eder. Saldırgan ne kadar fazla paket gönderirse, yakalanma riski o kadar artar.

"Mükemmel Suç Yoktur, Sadece İncelenmemiş Log Vardır"

Bu hafta Ann'in AIM trafiğini analiz ettik. **Her şey pcap'te açıkça duruyordu:**

- Kiminle konuştu → Buddy Name
- Ne gönderdi → recipe.jpg
- İçerik ne → Açık metin, şifresiz!

Ann "kimse fark etmez" diye düşündü ama **ağ her şeyi kaydetti.**

Saldırganlar "mükemmel plan" yaparlar ama **teknik gerçek şu:** Her paket, her bağlantı, her login **iz bırakır.** Fark edilmemelerinin tek sebebi **kimsenin bakmamış olması.**

Eğer güvenlik ekibi pcap'i açıp inceleseydi, Ann ilk mesajdan yakalanırdı. Sorun saldırganın zekası değil, **savunmanın dikkatsizliği.**

Sonuç: Log toplamak yetmez, **analiz etmek** gerekir. Çoğu ihlal, aylarca sistemde kalır çünkü kimse loglara bakmaz. "Mükemmel suç" diye bir şey yok