

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 iletişimini, 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 içerisindeki hastanın isim, soy isim yani Log ama doktor içerisindeki 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 düşünebiliriz. 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 gereklidir ama şifreyi çözemediğinden kendince yeni şifre yapar, bilgisayarı ya da sunucuyu taklit ederek sahte sertifika yani şifreyi biliyormuş gibi davranış gösterir 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 iletişimini keser bu da Wireshark'ta yarı kalmış kırmızı bağlantılar neden olur. Normal iletişimde aynı anda max iki kapı kullanır ama Taramada aynı anda birsürü kapı kullandığını görürsün. Normal iletişimde 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 sırada başka müşterilerin oda istediğini ama boş odanın kalmadığını söylemen gibi bir şevidir. TCP bağlantısı kurulana kadar bağlantı bilgilerini Backlog Queue belleğinde tutar ama bellekte ayrılan yer sınırlıdır. Ayrılan yer dolunca yarı açık bağlantı kuyruğu kilitlenir.

BÖLÜM B

1. Arayüz ve Renkler

No.	Time	Source	Destination	Protocol	Length Info
2709	19.096592	196.196.53.11	10.60.212.96	TCP	56 57219 → 63201 [RST]
2710	19.104632	10.60.212.96	86.155.246.195	TCP	66 [TCP Retransmission]
2711	19.104738	10.60.212.96	181.41.206.153	TCP	66 [TCP Retransmission]
2712	19.104754	10.60.212.96	45.43.99.77	TCP	66 [TCP Retransmission]
2713	19.104768	10.60.212.96	69.16.157.245	TCP	66 [TCP Retransmission]
2714	19.105352	10.60.212.96	216.58.214.142	UDP	1292 52595 → 443 Len=12
2715	19.120463	10.60.212.96	52.108.24.0	TCP	1434 [TCP Retransmission]
2716	19.122261	216.58.214.142	10.60.212.96	UDP	73 443 → 52595 Len=31
2717	19.123026	10.60.212.96	216.58.214.142	UDP	1292 52595 → 443 Len=12
2718	19.152981	10.60.212.96	216.58.214.142	UDP	1292 52595 → 443 Len=12
2719	19.174055	216.58.214.142	10.60.212.96	UDP	74 443 → 52595 Len=32

Frame 2711: Packet, 66 bytes on wire (528 bits), 0000 00 00 0c 9f f1 d8 88 f4 da 43 2f 5b 08 00 45
Ethernet II, Src: Intel_43:2f:5b (88:f4:da:43:2f:
Internet Protocol Version 4, Src: 10.60.212.96, D:
Transmission Control Protocol, Src Port: 63200, D:
0010 00 34 e9 57 40 00 80 06 00 00 0a 3c d4 60 b5
0020 ce 99 f6 e0 6b 98 91 7d 79 a5 00 00 00 00 80
0030 ff ff 62 86 00 00 02 04 05 b4 01 03 03 08 01
0040 04 02

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.

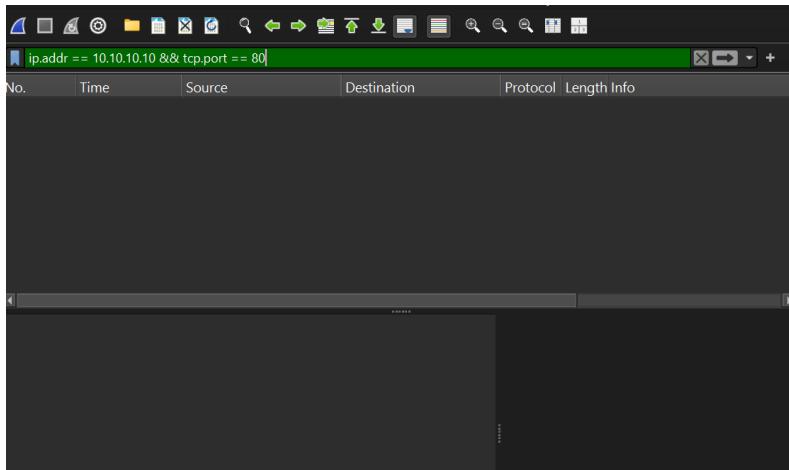
Internet Protocol : Ağ katmanı , paketin IP adresini gösterir.

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 Destination (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.

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Tr...
2	3.003255	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Tr...
3	6.006239	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Tr...
4	14.641385	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery I...
5	19.646175	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery I...
6	23.595917	HuaweiTechno_f0:45:d7	Sfr_e3:c3:31	ARP	60 Who has 10.251.196...
7	23.595953	HuaweiTechno_f0:45:d7	Sfr_60:2d:11	ARP	60 Who has 10.194.144...
8	24.651131	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery I...
9	29.254270	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Tr...
10	29.811743	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery I...
11	32.257198	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Tr...
12	32.771702	HuaweiTechno_f0:45:d7	Sfr_e3:c3:31	ARP	60 Who has 10.194.144...

Frame 6: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) 0000 30 7e cb e3 c3 31 80 ...
Ethernet II, Src: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7), Dst: Sfr_e3:c3 0010 08 00 06 04 00 01 80
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7)
Sender IP address: 10.251.196.1
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 10.251.196.227

Opcodes (arp.opcode), 2 byte(s) Paketler: 531 Profil: Default

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

No.	Source	Destination	Protocol	Length Info
00000	145.254.160.237	65.208.228.223	TCP	62 3372 → 80 [SYN] Seq=0 Win=8760 Len=0
11310	65.208.228.223	145.254.160.237	TCP	62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
	65.208.228.223	145.254.160.237	TCP	62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
	145.254.160.237	65.208.228.223	TCP	54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0

Sorguları (Görev 10: DNS Trafiği)

Sorgu paketi UDP protokolu ile gider.

6. DNS

145.254.160.237	145.253.2.203	DNS	89 Standard query 0x0023 A pagead2.googlesyndication.com
65.208.228.223	145.254.160.237	TCP	1434 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432
145.254.160.237	65.208.228.223	TCP	54 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660
65.208.228.223	145.254.160.237	TCP	1434 80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432
Frame 13: Packet, 89 bytes on wire (712 bits), 89 bytes captured (712 bits)			
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)			
Destination: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)			
.... .1. = LG bit: Locally administered address (this is NOT the factory default)			
.... .0. = IG bit: Individual address (unicast)			
Source: Xerox_00:00:00 (00:00:01:00:00:00)			
.... .0. = LG bit: Globally unique address (factory default)			
.... .0. = IG bit: Individual address (unicast)			
Type: IPv4 (0x0800)			
[Stream index: 0]			
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 145.253.2.203			
User Datagram Protocol, Src Port: 3009, Dst Port: 53			

7. HTTP vs HTTPS (Görev 11 ve 12)

4 0.911310	145.254.160.237	65.208.228.223	HTTP	533 GET /download.html
5 1.472116	65.208.228.223	145.254.160.237	TCP	54 80 → 3372 [ACK] Seq=1 Ack=1 Len: 479
6 1.682419	65.208.228.223	145.254.160.237	TCP	1434 80 → 3372 [ACK] Seq=2 Ack=1 Len: 479
7 1.812606	145.254.160.237	65.208.228.223	TCP	54 3372 → 80 [ACK] Seq=1 Ack=2 Len: 479
8 1.812606	65.208.228.223	145.254.160.237	TCP	1434 80 → 3372 [ACK] Seq=2 Ack=1 Len: 479
9 2.012894	145.254.160.237	65.208.228.223	TCP	54 3372 → 80 [ACK] Seq=1 Ack=2 Len: 479
10 2.443513	65.208.228.223	145.254.160.237	TCP	1434 80 → 3372 [ACK] Seq=2 Ack=1 Len: 479
11 2.553672	65.208.228.223	145.254.160.237	TCP	1434 80 → 3372 [PSH, ACK] Seq=3 Ack=1 Len: 479
12 2.553672	145.254.160.237	65.208.228.223	TCP	54 3372 → 80 [ACK] Seq=1 Ack=3 Len: 479
13 2.553672	145.254.160.237	145.253.2.203	DNS	89 Standard query 0x0023 A pagead2.googlesyndication.com
Frame 4: Packet, 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)				
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)				
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223				
Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479				
Hypertext Transfer Protocol				
GET /download.html HTTP/1.1\r\n				
Host: www.ethereal.com\r\n				
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n				
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,image/*,image/*				
Accept-Language: en-us,en;q=0.5\r\n				
Accept-Encoding: gzip,deflate\r\n				
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n				
Paketler: 43				Profil: Default

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

No.	Time	Source	Destination	Protocol	Length Info
2 0.660801	192.168.100.1	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1	
3 1.662661	192.168.100.1	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1	
4 2.665708	192.168.100.1	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1	
5 3.031646	192.168.100.128	54.193.240.194	OpenVPN	158 MessageType: P_DAT	
6 3.665770	192.168.100.1	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1	
7 5.880142	54.193.240.194	192.168.100.128	OpenVPN	158 MessageType: P_DAT	
8 5.980996	192.168.100.128	192.168.100.6	TCP	74 60368 → 135 [SYN]	
9 5.981332	VMware_fc:eb:3a	Broadcast	ARP	42 Who has 192.168.100.128	
10 5.981663	VMware_fc:eb:3a	VMware_fc:eb:3a	ARP	60 192.168.100.128 is	
11 5.981737	192.168.100.6	192.168.100.128	TCP	66 135 → 60368 [SYN, ACK]	
12 5.982097	192.168.100.128	192.168.100.6	TCP	60 60368 → 135 [ACK]	
13 5.982538	192.168.100.128	192.168.100.6	DCERPC	126 Bind: call_id: 1, port: 114	
14 5.982638	192.168.100.6	192.168.100.128	DCERPC	114 Bind ack: call id: 1, port: 114	
Frame 8: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits)					
Ethernet II, Src: VMware_fc:4e:63 (00:0c:29:5f:4e:63), Dst: VMware_fc:eb:3a (00:0c:29:fc:eb:3a)					
Internet Protocol Version 4, Src: 192.168.100.128, Dst: 192.168.100.6					
Transmission Control Protocol, Src Port: 60368, Dst Port: 135, Seq: 0, Len: 0					
Source Port: 60368					
Destination Port: 135					
[Stream index: 0]					
[Stream Packet Number: 1]					
[Conversation completeness: Complete, WITH_DATA (31)]					
[TCP Segment Len: 0]					
Sequence Number: 0 (relative sequence number)					
Sequence Number (raw): 6588228025					
Paketler: 1171				Profil: Default	

Siyah satırı bakıldığından 192.168.100.128 IP adresine sahip cihazın saldırıcı 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 ağıda karışık mod açmamalıyız,IDS yüzünden izlenebilirliğiniz artar, meslekte güvensiz birine dönüşürsünüz, sabıka kaydınız çalışmaya 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 değiştir 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 saldırımı bulabiliriz.