

Görev 2: Paket Dedektiflik Raporu

BÖLÜM A: Teori ve İspat

1.Meekanik ve Altyapı:

Token Ring (Tring) , yerel alan ağları oluşturmak için kullanılan fiziksel ve veri bağlantı katmanı bilgisayar ağ teknolojisidir

Frame Relay anahtarlanmış paket teknolojisine dayanmaktadır. Veriyi küçük paketlere bölerek gönderir. Bu paketler Frame olarak adlandırılır. Bu paketler gönderilecek olan adresi, gönderenin adresini ve orijinal mesajın bir parçasını içerir. Frame Relay'de, iletilen paketler için iletim sırasında herhangi bir anda hata kontrolü yapılmaz. Verinin iletileceği nokta hata kontrolünden sorumludur. Bunun sonucunda, paket iletim hızları çok yüksektir.

Karışık (gelişigüzel) mod: Ağ üzerindeki tüm paketleri görebilmek için Wireshark'ta aktif edilen moddur. Normalde bir ağ kartı sadece kendisine ait olan trafiği işler ancak karışık mod açıkken ağ kartı(NIC) hedef MAC adresine bakmadan tüm paketleri üst katmanlara iletir. Bu mod kapalı olunca NIC sadece hedef MAC adreslerine gönderilen paketleri, broadcast(yayın) ve multicast(çoklu yayın) paketlerini iletir.

Switch ve Hub: Switch ve Hub bilgisayarların birbirleriyle iletişim kurmasını sağlayan cihazlardır. Switch , veri aktarılan bilgisayar ile veriyi alan bilgisayar arasında iletişim kurulmasını sağlar. Hedef adresi bilen Switch'ler verileri portlar aracılığıyla aktarmak istenilen bilgisayara kolayca aktarır. Hub, birbirine bağlı cihazların veri iletimini sağlar. Aynı ağdaki bilgisayarlar veri alışverişi yaptığında bveri iletimini sağlayan cihaz Hub'dır. İkisi de veri iletimi sağlayan cihazların birbirinden farklarına değinecek olursak Switch cihazı programlanabilirken Hub cihazı programlanamaz.

Switch cihazı anahtarlama yöntemi ile çalışırken Hub cihazı ise yayın haberleşme özelliğine sahiptir.

Hub cihazında bant genişliği tüm cihazlara bölünür, paylaşılır ama Switch te böyle bir durum söz konusu değildir. Switch daha güvenilir bir sistemdir. Switch cihazının kullanıldığı ağda başkasının veri iletimi, şeması görülebilir mi ? Evet , görülebilir. Broadcast trafiği tüm portlara gider, eğer hedef MAC adresi bilinmiyorsa veri ilk başta tüm portlara gider , Switch üzerinden özel olarak bir port diğer porta kopyalanabilir, yapılandırılabilir. Bunlardan başka bir yol olarak da saldırganlar ARP Spoofing yani 2 cihaz arasına girerek yapar. LAN üzerinden gerçekleşen ve IP ile MAC adres tablosuna kötü amaçlı ARP paketleri gateway e göndererek saldırılarını gerçekleştirir. ARP protokolü IP adresini MAC adresine çevirir. Saldırgan varsayılan ağ geçidine ARP yanıt

mesajı göndererek mac adresinin hedefinin IP adresiyle ya da tam tersinin ilişkilendirilmesi gerektiğini bildirerek 2 cihaz arasına girerek iletilen verileri görebilir hatta değiştirebilir.

PCAP vs Log: Log(firewall daki); kaynak IP, hedef IP, port, zaman gibi bilgilerin tutulduğu dosyalardır.

PCAP dosyası, paket yakalama sırasında yakalanan ağ trafiğini depolamak için kullanılan kaynak ve hedef IP adresleri, yük verileri, zaman gibi bilgileri içeren veri dosyasıdır. Bir olay müdahalesinde yorum içermeyen, gerçek veriyi gösteren, payload analizi yapan PCAP kesin delil olarak sayılır.

2.Protokol Anatomisi:

3--Way Handshake(Üçlü El Sıkışma):

SYN(senkronizasyon): İstemci, sunucuya bir bağlantı isteği gönderir. (Yeni öğrenci:Merhaba, ben yeni öğrenciyim kayıt oluşturmak istiyorum içeri gelebilir miyim?)

SYN-ACK(senkronizasyon- onay): Sunucu isteğini alır ve hazır olduğunu bildirir.(Müdür: Merhaba, tabii kayıt oluşturmak için içeri girebilirsin .)

ACK(onay): İstemci , sunucunun hazır olduğunu anlar ve veri akışı başlar.(öğrenci kaydı oluşturulur. öğrenci bilgilerini müdüre verir ve kayıt oluşur.)

TCP vs UDP: TCP UDP'ye göre daha fazla bant genişliği kullanır ve daha yavaştır çünkü verinin karşı tarafa ulaşp ulaşmadığını kontrol eder. UDP ise TCP ye göre daha güvensiz bir protokoldür. TCP verilerin sırasıyla iletilmesini sağlar.TCP 2 cihaz arasındaki bağlantı kesine hale geldikten sonra verileri iletir.UDP ise bağlantı kurmadan veri gönderir. Bir paket kaybı olursa TCP protokolü o paketi yeniden iletmeye çalışır. Ancak UDP yeniden iletmez.

Sıra Numarası: Hedef bilgisayarın , verileri sırasıyla işleyebilmesi için paketlere numaralar verilir. TCP protokolü eğer paket iletiminde eksiklik olursa o paketi tekrar gönderir. Eğer 5. paket 3. paketten önce gelirse sırası gelene kadar 5. paket bekletilir (buffer).

3. Kimlik ve Adresleme

ARP Protokolü (kimde vardır?):ARP protokolü ağ anahtarı sadece MAC adresini tanıdığından MAC adresine duyarlıdır. IP adreslerini MAC adresleriyle eşleştirerek IP adreslerinden gelen veri iletimi isteği de bu sayede gerçekleşir.

DHCP adresi(DORA süreci): Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP), IP adreslerinin ve diğer ağ yapılandırma ayarlarının bir ağdaki cihazlara otomatik olarak atanmasını sağlayan bir ağ protokolüdür. DHCP süreci DORA 4 adımın kısaltmasıdır , keşfet, teklif, istek, onay aşamalarından oluşur. Discover adımı, ağa yeni dahil olan cihaz, ortamdaki DHCP sunucularını belirlemek için tüm ağa bir yayın (broadcast) paketi gönderir. bu şekilde DHCP sunucusu ve IP adresi ataması talep eder.

Offer, discover mesajına cevap olarak teklif mesajıyla DHCP sunucusunun istemciye atamak istediği IP yi içerir. Request(talep): İstemci teklif mesajlarından birini seçip sunulan IP adresini kabul ettiğini onaylar. Accept(onay) adımı DHCP sunucusu istemciye onay mesajı gönderir. Bu onayla IP ataması sonlanır.

DNS: Tarayıcıya google.com yazıldığında bilgisayar bu adresin ne olduğunu anlamak için DNS sunucusuna gidilir ve DNS sunucusu bu alan adını IP e çevirir bu şekilde tarayıcı internet kaynağına ulaşır.

4. Şifreleme ve Kör noktaları:

HTTPS ve Şifreleme: Wireshark ile şifreli bir paket yakalandığında kullanıcı adı, şifre gibi hassas bilgiler gizli kalabilir ancak IP adresi, port, SNI gibi bilgiler gözükür.

Ortadaki Adam: Şifreli bir tünel doğrudan kırılmadığından saldırganlar hedeflerine sahte anahtar(sertifika) verirler. Kendilerini farklı tanıtarak kişinin verilerini çalarlar.

5. Saldırı İmzaları:

Port taraması: Normal iletim belirli bir portta, TCP adımları gerçekleşerek , veri paketleri gelir, bağlantı düzgün kapanır . Port taramasında kısa zamanda çok sayıda porttan , TCP adımları tamamlanmadan, RST yoğunluğu gözlenerek iletim gerçekleşir.

Hizmet Reddi: Bir sunucuya 100.000 SYN gönderilirse sunucu hepsine SYN-ACK adımını gerçekleştirir ancak saldırgan ACK paketini göndermeyerek sunucuda bekleyen SYN-ACK ler bağlantı istekleri bekleme listesini doldurur ve gerçek bir talebe cevap veremez duruma gelir. Sistem kitlenir.

BÖLÜM B: Saha Eğitimi ve Araç Hakimiyeti

1. Arayüz ve Renkler:

OSI modelinin 2. Katmanında veri iletimi katmanı vardır. MAC adreslerinin olduğu yerdir buradaki

destination (hedef) , : 5c:b4:7e:9a:a8:03 source (kaynak) : cc:29:bd:f2:3d:05 adreslerini fiziksel olarak içerir. Ethernet II 3. Katmanda ise ağ katmanı yer alır. Bu katmanda

source(IP): 140.82.113.26 ve destination: 192.168.1.105 mantıksal adreslerini içerir.4.Katman ise taşıma katmaıdır buraya ait bilgilere bakacak olursak src port: 443 dst port: 64972 sıra numarası: 26 onay numarası: 30 dur.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	18.97.36.58	192.168.1.105	TLSv1.2	78	Application Data
2	0.001074	192.168.1.105	18.97.36.58	TLSv1.2	82	Application Data
3	0.041117	140.82.113.26	192.168.1.105	TLSv1.2	79	Application Data
4	0.041644	192.168.1.105	140.82.113.26	TLSv1.2	83	Application Data
5	0.205917	18.97.36.58	192.168.1.105	TCP	54	443 → 56934 [ACK] Seq=25 Ack=29 Win=1228
6	0.205917	140.82.113.26	192.168.1.105	TCP	54	443 → 64972 [ACK] Seq=26 Ack=30 Win=76 Len=0
7	0.205917	35.201.82.116	192.168.1.105	UDP	93	443 → 55961 Len=51
8	0.240269	192.168.1.105	35.201.82.116	UDP	74	55961 → 443 Len=32
9	0.383377	fe80::5567:fe31:5b5...	fe80:::1	DNS	103	Standard query 0x5c63 A www.msftconnectte
10	0.383408	fe80::5567:fe31:5b5...	fe80:::1	DNS	104	Standard query 0x7bc1 A ipv6.msftconnectte
11	0.383711	fe80::5567:fe31:5b5...	fe80:::1	DNS	104	Standard query 0xfb4f AAAA ipv6.msftconne
12	0.384016	fe80::5567:fe31:5b5...	fe80:::1	DNS	103	Standard query 0x518d AAAA www.msftconne
13	0.411150	fe80:::1	fe80::5567:fe31:5b5...	DNS	247	Standard query response 0x5c63 A www.msft
14	0.411150	fe80:::1	fe80::5567:fe31:5b5...	DNS	289	Standard query response 0x7bc1 A ipv6.ms
15	0.411150	fe80:::1	fe80::5567:fe31:5b5...	DNS	284	Standard query response 0xfb4f AAAA ipv6.
16	0.411150	fe80:::1	fe80::5567:fe31:5b5...	DNS	274	Standard query response 0x518d AAAA www.m
17	0.413079	192.168.1.105	184.24.77.30	TCP	66	61498 → 80 [SYN] Seq=0 Win=65535 Len=0 MS
18	0.413435	2a00:1d34:3c37:2e00...	2a02:26f0:dc::6853:...	TCP	86	61499 → 80 [SYN] Seq=0 Win=65535 Len=0 MS
19	0.459363	2407:30c0:182::aa72...	2a00:1d34:3c37:2e00...	TCP	74	443 → 63744 [ACK] Seq=1 Ack=1 Win=16 Len=
20	0.459459	2a00:1d34:3c37:2e00...	2407:30c0:182::aa72...	TCP	74	[TCP ACKed unseen segment] 63744 → 443 [
21	0.460655	184.24.77.30	192.168.1.105	TCP	66	80 → 61498 [SYN, ACK] Seq=0 Ack=1 Win=64
22	0.460871	192.168.1.105	184.24.77.30	TCP	54	61498 → 80 [ACK] Seq=1 Ack=1 Win=65280 Le
23	0.461273	192.168.1.105	184.24.77.30	HTTP	165	GET /connecttest.txt HTTP/1.1
24	0.477826	2a02:26f0:dc::6853:...	2a00:1d34:3c37:2e00...	TCP	86	80 → 61499 [SYN, ACK] Seq=0 Ack=1 Win=64
25	0.478034	2a00:1d34:3c37:2e00...	2a02:26f0:dc::6853:...	TCP	74	61499 → 80 [ACK] Seq=1 Ack=1 Win=65280 Le

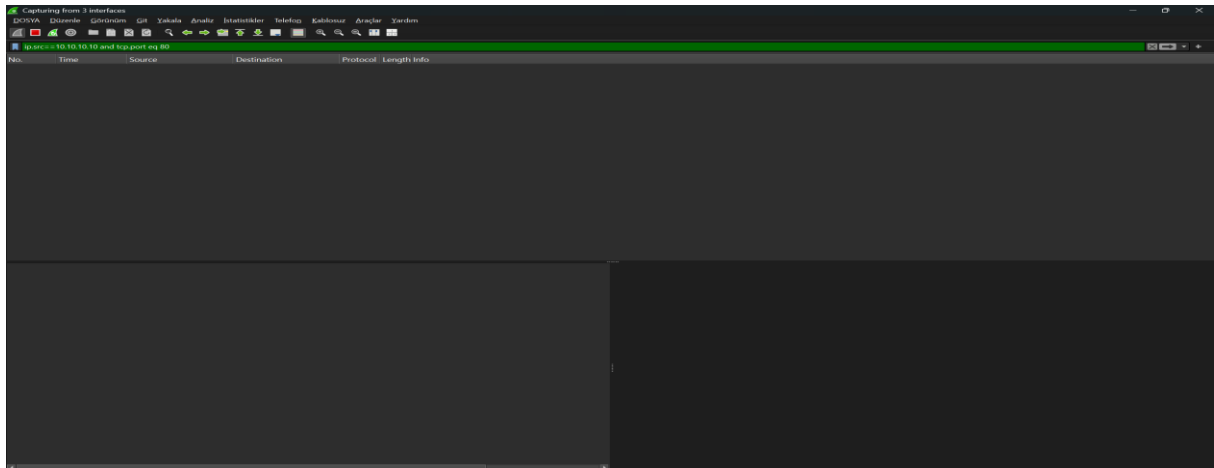
▶ Frame 6: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{CE8E8C5A-0451-4...
 ▶ Ethernet II, Src: zte_f2:3d:05 (cc:29:bd:f2:3d:05), Dst: Intel_9a:a8:03 (5c:b4:7e:9a:a8:03)
 ▶ Internet Protocol Version 4, Src: 140.82.113.26, Dst: 192.168.1.105
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 64972, Seq: 26, Ack: 30, Len: 0

Görseldeki siyah ve kırmızıyla yazılı satır ve görselde yok ancak arka planı kırmızı olan satırlar ağdaki paket iletiminde sorun olduğunun işaretidir. Paket ulaşmamış olabilir, bağlantı aniden kesilmiş olabilir, sırayla gitmeyen veriler olabilir.

2.Filtreleme Sanatı:

Görev : ip.src== 10.10.10.10 and tcp.port eq 80

Kanıt:



3.OSI ile Paket ilişkisi

Soru: MAC e aittir. Çünkü Ethernet II 2. Katmandır. Ve burada source ve destination a fiziksel olarak ulaşılabilir. IP adresi için 3. Katman olmalıdır.

4.ARP Trafiği Görevi

Soru: Opcode(1): soru; Opcode(2): cevap anlamına gelir.

Kanıt:

Time	Source	Destination	Protocol	Length	Info
1 0.000000	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Transaction ID 0x6f5114eb
2 3.003255	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Transaction ID 0x6f5114eb
3 6.006239	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Transaction ID 0x6f5114eb
4 14.641385	e0:a1:d7:18:c2:73	ff:ff:ff:ff:ff:ff	PPPoE	82	Active Discovery Initiation (PADI)
5 19.646175	e0:a1:d7:18:c2:73	ff:ff:ff:ff:ff:ff	PPPoE	82	Active Discovery Initiation (PADI)
6 23.595917	80:fb:06:f0:45:d7	30:7e:cb:e3:c3:31	ARP	60	Who has 10.251.196.227? Tell 10.251.196.1
7 23.595953	80:fb:06:f0:45:d7	30:7e:cb:60:2d:11	ARP	60	Who has 10.194.144.144? Tell 10.194.144.1
8 24.651131	e0:a1:d7:18:c2:73	ff:ff:ff:ff:ff:ff	PPPoE	82	Active Discovery Initiation (PADI)
9 29.254270	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Transaction ID 0x656db7d
10 29.811743	e0:a1:d7:18:c2:73	ff:ff:ff:ff:ff:ff	PPPoE	82	Active Discovery Initiation (PADI)
11 32.257198	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Transaction ID 0x656db7d
12 32.771702	80:fb:06:f0:45:d7	e0:a1:d7:49:6d:f9	ARP	60	Who has 10.194.144.84? Tell 10.194.144.1
13 32.772685	80:fb:06:f0:45:d7	02:26:44:f0:cf:e8	ARP	60	Who has 10.194.144.147? Tell 10.194.144.1
14 32.774163	80:fb:06:f0:45:d7	c0:ac:54:17:e0:c9	ARP	60	Who has 10.251.196.162? Tell 10.251.196.1
15 34.816127	e0:a1:d7:18:c2:73	ff:ff:ff:ff:ff:ff	PPPoE	82	Active Discovery Initiation (PADI)
16 35.260227	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Transaction ID 0x656db7d
17 37.765789	80:fb:06:f0:45:d7	30:7e:cb:72:0a:d9	ARP	60	Who has 10.251.196.132? Tell 10.251.196.1
18 37.767245	80:fb:06:f0:45:d7	30:7e:cb:97:24:91	ARP	60	Who has 10.251.196.106? Tell 10.251.196.1
19 37.768724	80:fb:06:f0:45:d7	30:7e:cb:88:e7:a1	ARP	60	Who has 10.251.196.74? Tell 10.251.196.1
20 39.821132	e0:a1:d7:18:c2:73	ff:ff:ff:ff:ff:ff	PPPoE	82	Active Discovery Initiation (PADI)
21 39.874293	00:17:33:61:00:00	e0:a1:d7:18:c2:73	PPPoE	64	Active Discovery Offer (PADO) AC-Name='SE
22 39.874692	e0:a1:d7:18:c2:73	00:17:33:61:00:00	PPPoE	82	Active Discovery Request (PADR)
23 39.875775	00:30:88:03:a4:3b	e0:a1:d7:18:c2:73	PPPoE	64	Active Discovery Offer (PADO) AC-Name='SE
24 40.024585	00:17:33:61:00:00	e0:a1:d7:18:c2:73	PPPoE	64	Active Discovery Session-confirmation (PA
25 40.048828	e0:a1:d7:18:c2:73	00:17:33:61:00:00	PPP LCP	36	Configuration Request

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

5.TCP El Sıkışması

Görev:Trafikte 3-way handshake sürecinde bulun.

Kanıt:

7	1.391734	2a00:1d34:3c37:2e00::2603:1063:27:2:14	TLSv1.3	971	1464186612 Client Hello (SNI=ecs.office.com)
8	1.398330	2603:1063:27:2:14	TCP	74	3067123802 443 → 55248 [ACK] Seq=1 Ack=898 Win=4193280 Len=0
9	1.398330	2603:1063:27:2:14	TLSv1.3	362	3067123802 Server Hello, Change Cipher Spec, Application Data
10	1.398437	2a00:1d34:3c37:2e00::2603:1063:27:2:14	TCP	74	1464187509 55248 → 443 [ACK] Seq=898 Ack=289 Win=261632 Len=0
11	1.401020	2a00:1d34:3c37:2e00::2603:1063:27:2:14	TLSv1.3	154	1464187509 Change Cipher Spec, Application Data
12	1.401398	2a00:1d34:3c37:2e00::2603:1063:27:2:14	TLSv1.3	708	1464187509 Application Data
13	1.407446	2603:1063:27:2:14	TCP	74	3067124090 443 → 55248 [ACK] Seq=289 Ack=978 Win=4193280 Len=0
14	1.407446	2603:1063:27:2:14	TCP	74	3067124090 443 → 55248 [ACK] Seq=289 Ack=1612 Win=4194304 Len=0
15	1.637157	2603:1063:27:2:14	TLSv1.3	945	3067124090 Application Data
16	1.637317	2a00:1d34:3c37:2e00::2603:1063:27:2:14	TCP	74	1464188223 55248 → 443 [ACK] Seq=1612 Ack=1160 Win=260864 Len=0
17	2.466381	2a00:1d34:3c37:2e00::2a00:1450:4017:812:...	TCP	75	1484166108 63806 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1

6.DNS Sorguları:

Soru: Veri küçük olduğundan DNS sorgusu UDP protokolüne gider. İşlem hızlı gerçekleşir.

Kanıt:

The image shows a Wireshark capture of a network packet. The top pane displays a list of captured packets. The selected packet is a DNS query (No. 89, Time 19.705358, Source fe80::1, Destination fe80::5567:fe31:5b5...). The middle pane shows the packet details, including Ethernet II, Internet Protocol Version 6, and User Datagram Protocol. The bottom pane shows the packet bytes.

No.	Time	Source	Destination	Protoc	Length	Sequence Number (raw)	Info
1	0.000000	VestelElektr_f7:46:...	Broadcast	ARP	42		Who has 192.1
309	28.257870	zte_f2:3d:05	Intel_9a:a8:03	ARP	46		Who has 192.1
310	28.257895	Intel_9a:a8:03	zte_f2:3d:05	ARP	42		192.168.1.105
84	19.702747	fe80::5567:fe31:5b5...	fe80::1	DNS	94		Standard quer
85	19.702823	fe80::5567:fe31:5b5...	fe80::1	DNS	94		Standard quer
88	19.705358	fe80::1	fe80::5567:fe31:5b5...	DNS	122		Standard quer
89	19.705358	fe80::1	fe80::5567:fe31:5b5...	DNS	110		Standard quer
129	23.083473	fe80::5567:fe31:5b5...	fe80::1	DNS	110		Standard quer
130	23.083601	fe80::5567:fe31:5b5...	fe80::1	DNS	110		Standard quer
131	23.090609	fe80::1	fe80::5567:fe31:5b5...	DNS	231		Standard quer
132	23.090843	fe80::1	fe80::5567:fe31:5b5...	DNS	307		Standard quer
151	23.713865	fe80::5567:fe31:5b5...	fe80::1	DNS	94		Standard quer
152	23.713984	fe80::5567:fe31:5b5...	fe80::1	DNS	94		Standard quer
153	23.714046	fe80::5567:fe31:5b5...	fe80::1	DNS	94		Standard quer
156	23.715743	fe80::5567:fe31:5b5...	fe80::1	DNS	100		Standard quer
157	23.715823	fe80::5567:fe31:5b5...	fe80::1	DNS	100		Standard quer
158	23.716046	fe80::5567:fe31:5b5...	fe80::1	DNS	100		Standard quer
162	23.722330	fe80::1	fe80::5567:fe31:5b5...	DNS	159		Standard quer
163	23.725361	fe80::1	fe80::5567:fe31:5b5...	DNS	110		Standard quer
164	23.725361	fe80::1	fe80::5567:fe31:5b5...	DNS	198		Standard quer
165	23.725973	fe80::1	fe80::5567:fe31:5b5...	DNS	149		Standard quer
180	23.728577	fe80::5567:fe31:5b5...	fe80::1	DNS	105	2099494092	Standard quer
182	23.728612	fe80::5567:fe31:5b5...	fe80::1	DNS	105	35111433	Standard quer
184	23.728645	fe80::5567:fe31:5b5...	fe80::1	DNS	105	690651961	Standard quer
203	23.793284	fe80::1	fe80::5567:fe31:5b5...	DNS	138	530320701	Standard quer

Frame 89: Packet, 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{CE8E8C5A-045...}

Ethernet II, Src: zte_f2:3d:05 (cc:29:bd:f2:3d:05), Dst: Intel_9a:a8:03 (5c:b4:7e:9a:a8:03)

Internet Protocol Version 6, Src: fe80::1, Dst: fe80::5567:fe31:5b52:85e4

User Datagram Protocol, Src Port: 53, Dst Port: 53531

Source Port: 53
Destination Port: 53531
Length: 56
Checksum: 0x7fe6 [unverified]
[Checksum Status: Unverified]
[Stream index: 6]
[Stream Packet Number: 2]
[Timestamps]
UDP payload (48 bytes)
Domain Name System (response)
Transaction ID: 0xe9fc
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
[Request In: 85]
[Time: 2.535000 milliseconds]

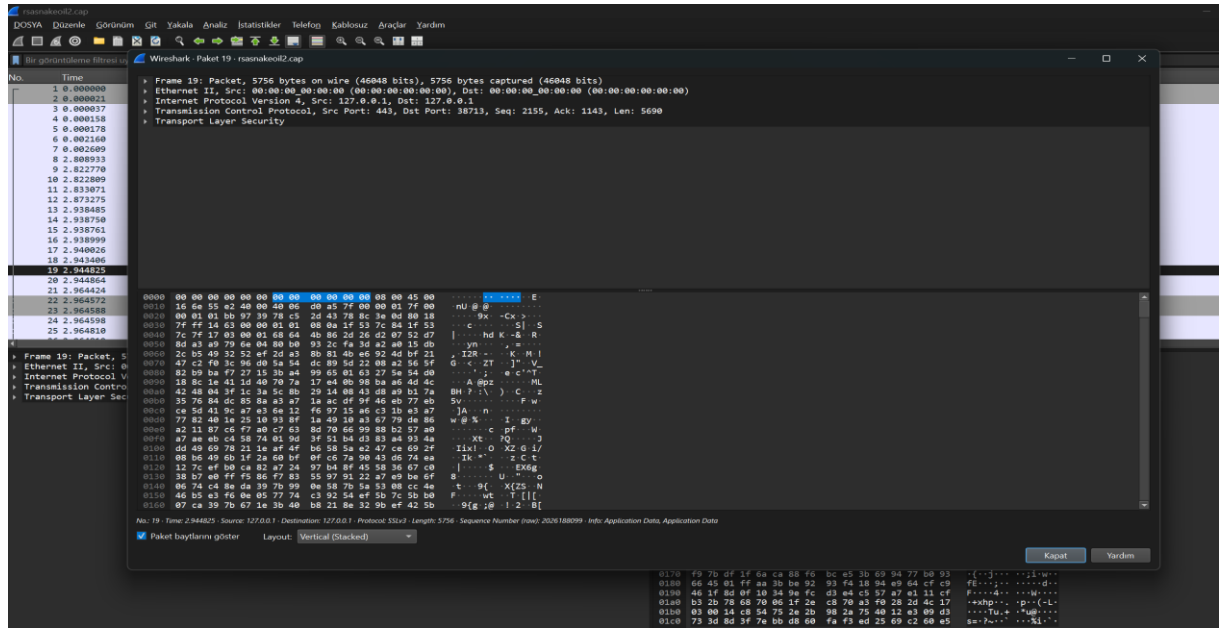
7.HTTP ve HTTPS

HTTP Analizi: POST isteğini göremedim.

The image shows a Wireshark capture of HTTP traffic. The top pane displays a list of captured packets. The selected packet is an HTTP GET request (No. 4, Time 0.911310, Source 145.254.160.237, Destination 65.208.228.223). The middle pane shows the packet details, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The bottom pane shows the packet bytes.

No.	Time	Source	Destination	Protocol	Length	Sequence Number (raw)	Info
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	951057940	GET /download.html HTTP/1.1
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	918691368	GET /pagead/ads/client=ca-pub-2309191948673629&random=108444343028581mt=1082467020&format=468x60_as&output=html&url=http%3A%2F%2Fwww...
38	4.846969	65.208.228.223	145.254.160.237	HTTP/XL	478	290236320	HTTP/1.1 200 OK
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	778787098	HTTP/1.1 200 OK (text/html)

HTTPS Analizi: Metin göremiyorum.



8.Saldırı Analizi:

Kanıt:

zerologon_160064822515.pcap							
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım							
Bir görüntüleme filtresi uygula ... <Ctrl-/>							
No.	Time	Source	Destination	Protocol	Length	Sequence Number (raw)	Info
25	5.987980	192.168.100.128	192.168.100.6	TCP	60	2297288359	57936 -> 49672
26	5.988451	192.168.100.128	192.168.100.6	DCERPC	126	2297288359	Bind: call_id
27	5.988584	192.168.100.6	192.168.100.128	DCERPC	114	4257177708	Bind_ack: cal
28	5.988875	192.168.100.128	192.168.100.6	TCP	60	2297288431	57936 -> 49672
29	5.990526	192.168.100.128	192.168.100.6	RPC_NE...	140	2297288431	NetrServerReq
30	5.990906	192.168.100.6	192.168.100.128	RPC_NE...	90	4257177768	NetrServerReq
31	5.991262	192.168.100.128	192.168.100.6	TCP	60	2297288517	57936 -> 49672
32	5.993544	192.168.100.128	192.168.100.6	RPC_NE...	174	2297288517	NetrServerAut
33	5.994367	192.168.100.6	192.168.100.128	RPC_NE...	98	4257177804	NetrServerAut
34	5.994738	192.168.100.128	192.168.100.6	TCP	60	2297288637	57936 -> 49672
35	5.995998	192.168.100.128	192.168.100.6	TCP	74	1240177321	60372 -> 135 [
36	5.996086	192.168.100.6	192.168.100.128	TCP	66	2538286178	135 -> 60372 [
37	5.996381	192.168.100.128	192.168.100.6	TCP	60	1240177322	60372 -> 135 [
38	5.996840	192.168.100.128	192.168.100.6	DCERPC	126	1240177322	Bind: call_id
39	5.996952	192.168.100.6	192.168.100.128	DCERPC	114	2538286179	Bind_ack: cal
40	5.997177	192.168.100.128	192.168.100.6	TCP	60	1240177394	60372 -> 135 [
41	5.999869	192.168.100.128	192.168.100.6	EPM	210	1240177394	Map request,
42	6.000205	192.168.100.6	192.168.100.128	EPM	206	2538286239	Map response,
43	6.000525	192.168.100.128	192.168.100.6	TCP	60	1240177550	60372 -> 135 [
44	6.002161	192.168.100.128	192.168.100.6	TCP	60	2297288637	57936 -> 49672
45	6.002245	192.168.100.6	192.168.100.128	TCP	54	4257177848	49672 -> 57936
46	6.002337	192.168.100.6	192.168.100.128	TCP	54	4257177848	49672 -> 57936
47	6.002618	192.168.100.128	192.168.100.6	TCP	60	2297288638	57936 -> 49672
48	6.003661	192.168.100.128	192.168.100.6	TCP	60	1240177550	60372 -> 135 [

Saldırgan hep aynı kaynaktan istek gelmesi ve farklı protokollerin gözlenmesiyle dikkat çekiyor.

