

[PENTEST LAB ÇALIŞMALARI]



# PENTEST EĞİTİMİ UYGULAMA KİTABI

## BÖLÜM - 3

## İÇİNDEKİLER

### 3. İNTERNET VE YEREL AĞ SIZMA TESTLERİ

#### BU KATEGORİDEKİ LAB UYGULAMA LİSTESİ

- 3.1. Iodine ile DNS Tünelleme
- 3.2. Cain&Abel Kullanarak ARP Cache Poisoning Saldırısı
- 3.3. DHCP Spoofing ve DHCP Resource Starvation Denemeleri
- 3.4. Paket Protokol Analizi Amaçlı Wireshark Kullanımı
- 3.5. Network Miner ile Trafik Analizi

### 3.1. Iodine ile DNS Tünelleme

**Amaç:** iodine programının kullanılarak DNS protokolü üzerinden internet erişim engellemelerinin aşılması.

**Kullanılan Araçlar:** iodine

**Uygulama:** iodine

Iodine açık kaynak ve desteği devam eden bir uygulamadır. Sunucu ve istemci mantığı ile çalışmaktadır. Özelleştirilmiş dns paketlerini kullanarak uzakta bulunan bir sunucu ile haberleşmek için kullanılmaktadır. Bu uygulama aynı zamanda bir saldırı aracı olarak kullanılmaktadır. İnternet erişiminin engellendiği bir yerel ağda, dns isteklerinin kısıtlanmaması durumunda, dns istekleri üzerinden internete çıkabilmeye olanak sağlamaktadır. Ayrıca ilgili ağda bulunan bilgileri dışarıya çıkarılması mümkün olmaktadır.

Iodine programı Kali Linux sistemlerde kurulu olarak gelmektedir. Ubuntu işletim sistemlerinde ise repository depolarında bulunmaktadır.

Sunucu tarafında iodine programı indirmek için;

```
apt-get install iodine
```

iodine sunucusunu yapılandırmak için

```
root@ub:~# iodined -f 10.0.0.1 v.sibercik.com -P tus
```

Burada verilen vpn.sibercik.com adresine dns kaydı girilmiştir. Hedef sunucu için bir dns kaydının girilmesi daha pratik olmaktadır.

İstemci tarafında girilmesi gereken komut;

```
iodine -P tus -T A 178.62.183.203 v.sibercik.com
```

Bu aşamada başarılı bir bağlantı kurulduktan sonra ifconfig komutu ile ağ arayüzleri görüntülendiğinde dns0 adında bir ağ arayüzünün sisteme eklendiği gözlemlenecektir.

```
root@kali:~# ifconfig
dns0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet addr:10.0.0.3  P-t-P:10.0.0.3  Mask:255.255.255.224
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1130  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:500
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth0    Link encap:Ethernet  HWaddr 00:0c:29:b2:93:5c
```

## [PENTEST LAB ÇALIŞMALARI]

```
inet addr:192.168.1.34 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:feb2:935c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:11231 errors:0 dropped:0 overruns:0 frame:0
TX packets:12631 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2329705 (2.2 MiB) TX bytes:1970042 (1.8 MiB)
```

```
lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:1
      RX packets:234 errors:0 dropped:0 overruns:0 frame:0
      TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:14060 (13.7 KiB) TX bytes:14060 (13.7 KiB)
```

Görüldüğü gibi 10.0.0.3 adresine sahip bir ağ arayüzü oluşturulmuş. Bu arayüz aracılığı ile 10.0.0.1 yani uzakta bulunan iodine suncusuna erişebilmek mümkün olacaktır.

```
root@kali:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_req=1 ttl=64 time=80.3 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=64 time=77.3 ms
```

Sunucu tarafında gelen trafik incelendiğinde ise;

```
root@ub:~# tcpdump -i dns0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on dns0, link-type RAW (Raw IP), capture size 65535 bytes
10:46:25.872259 IP 10.0.0.3 > 10.0.0.1: ICMP echo request, id 8016, seq 1, length 64
10:46:25.872315 IP 10.0.0.1 > 10.0.0.3: ICMP echo reply, id 8016, seq 1, length 64
10:46:26.887299 IP 10.0.0.3 > 10.0.0.1: ICMP echo request, id 8016, seq 2, length 64
10:46:26.887333 IP 10.0.0.1 > 10.0.0.3: ICMP echo reply, id 8016, seq 2, length 64
```

Gelen trafikte atılan ping istekleri görülmektedir.

### 3.2. Cain&Abel Kullanarak Arp Cache Poisoning Saldırısı

**Amaç:** Ağ güvenliği konusunda bazı protokollerin zayıf yönleri bulunmaktadır. Bu protokollerden biri ARP protokölüdür. Ortadaki adam saldırısı olarak bilinen “Man in the Middle(MITM)” saldırısında ARP protokolünün zayıflığı kullanılır. Local ağda bulunan başka bir bilgisayarın ağ trafiğini dinlenecektir.

**Lab Senaryosu:** Local ağda bulunan bir bilgisayarın ağ trafiğini dinleyebilmek için ARP Cache Poisoning yöntemi kullanılacaktır. Trafiği dinlenmek istenen bilgisayarın ile gateway arasına girilerek ortadaki adam saldırısı olarak bilinen “Man in the Middle(MITM)” gerçekleştirilecektir.

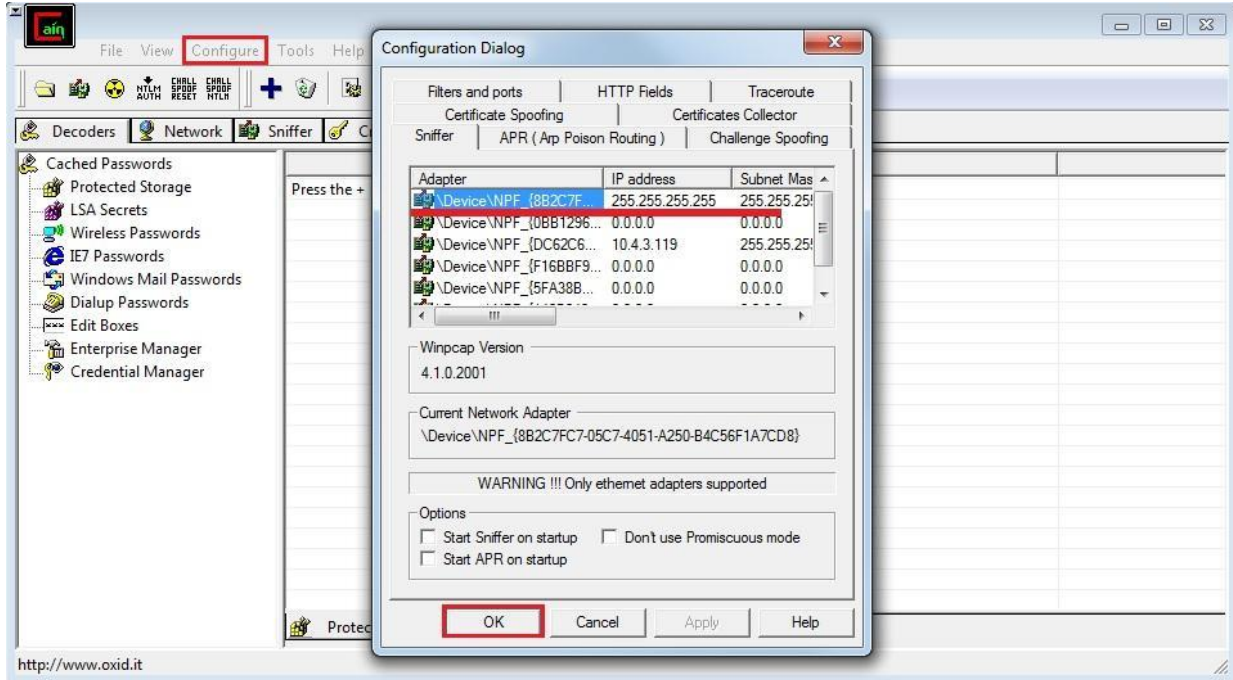
Gateway	PC - 01	PC - 02
192.168.2.1	192.168.2.2	192.168.2.6

- Kurban bilgisayarın(PC-02) arp tablosu kontrol edilir.

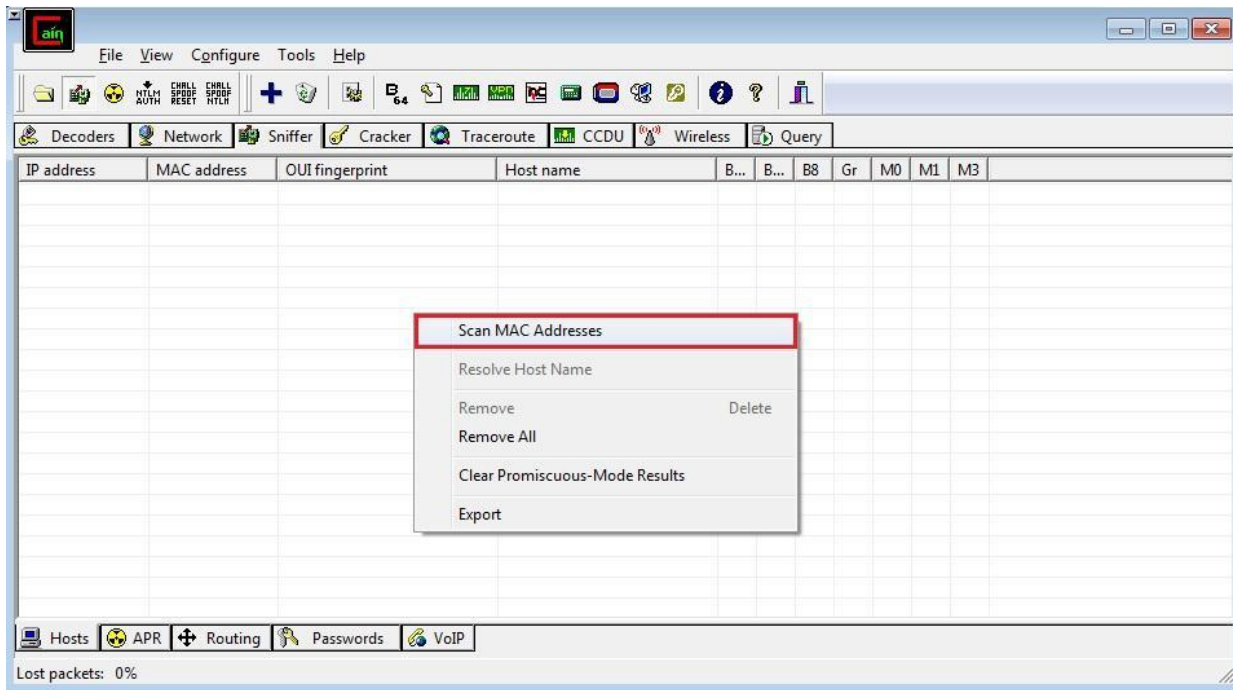
```
C:\Windows\system32>arp -a
Interface: 192.168.2.6 --- 0xc
Internet Address      Physical Address      Type
192.168.2.1          00-1c-a8-59-5e-25    dynamic
```

- Saldırı yapılacak bilgisayarda(PC-01) “Cain&Abel” programı çalıştırılır ve saldırı yapılacak ağ ara yüzü seçilir.

## [PENTEST LAB ÇALIŞMALARI]

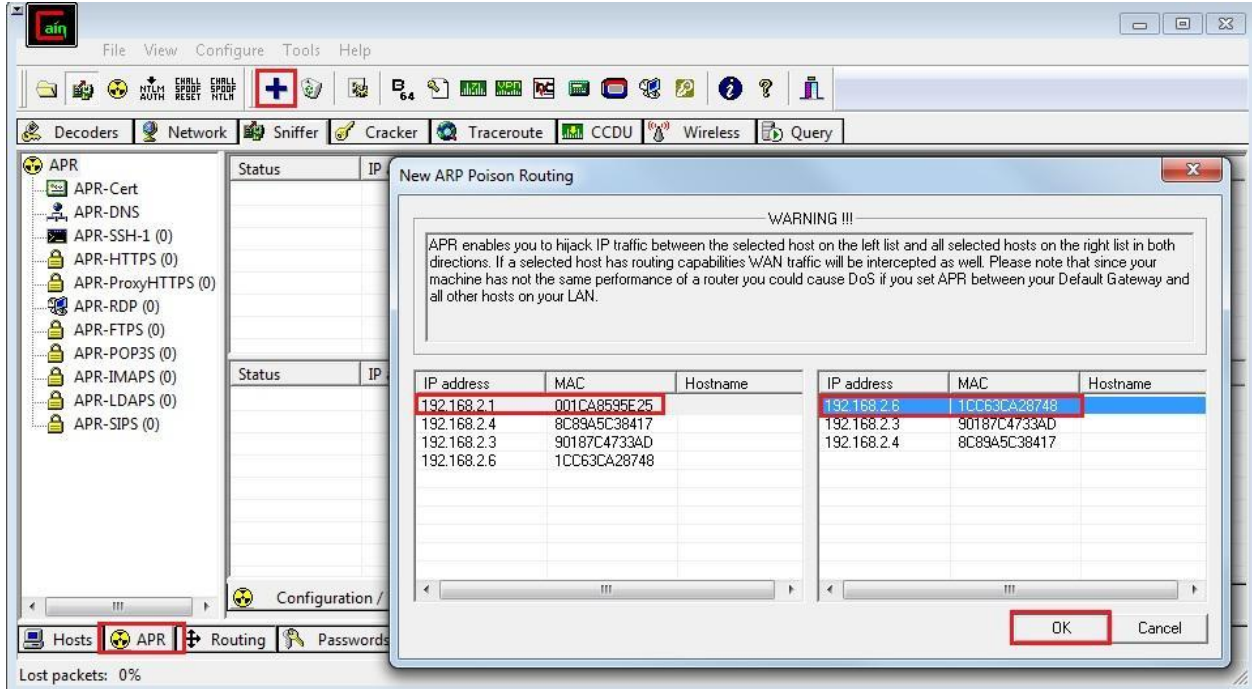


- Sniffer bölümünde yerel ağda bulunan aktif bilgisayarların keşfi yapılır. Programın orta kısmında farenin sağ düğmesine basılarak "Scan MAC Addresses" seçeneği seçilir ve isteğe göre ip aralığı ve tarama türleri belirtilerek keşif başlatılır.

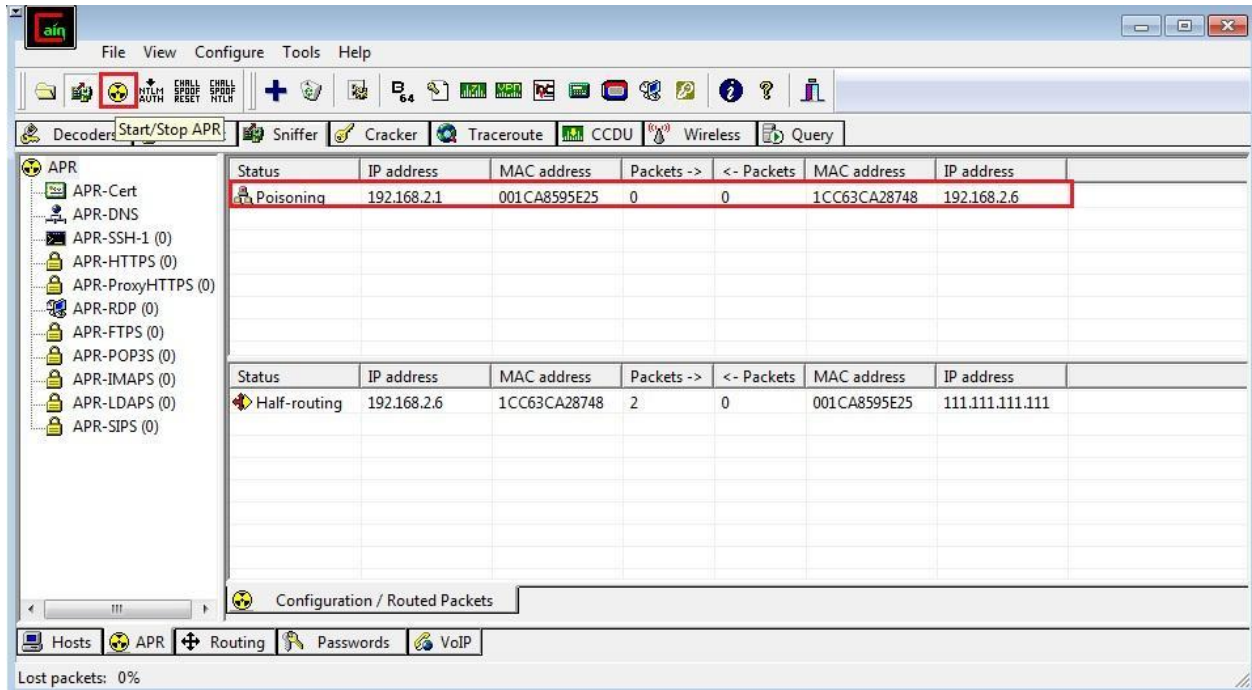


## [PENTEST LAB ÇALIŞMALARI]

- Sniffer altında bulunan "APR" bölümünde "+" düğmesine basarak kurban bilgisayarın çıkış kapısı ve kurban bilgisayarların ağ adresleri seçilir.



- Ağ zehirlenmesine başlanır ve kurban bilgisayarın(PC-02) arp tablosu tekrar kontrol edilir.



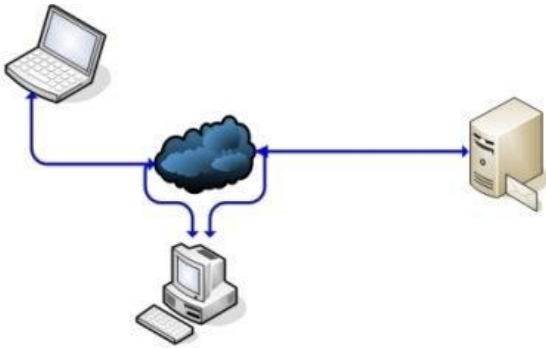
## [PENTEST LAB ÇALIŞMALARI]

- Zehirlenme işlemi sonrasında kurban bilgisayarın ARP tablosuna tekrar bakılır. Görüldüğü üzere çıkış kapısı (Gateway) MAC adresi değişmiş durumdadır. ARP tablosu zehirlenerek ağ trafiği saldırgan bilgisayar üzerinden geçecek şekilde devam ediyor olacaktır.

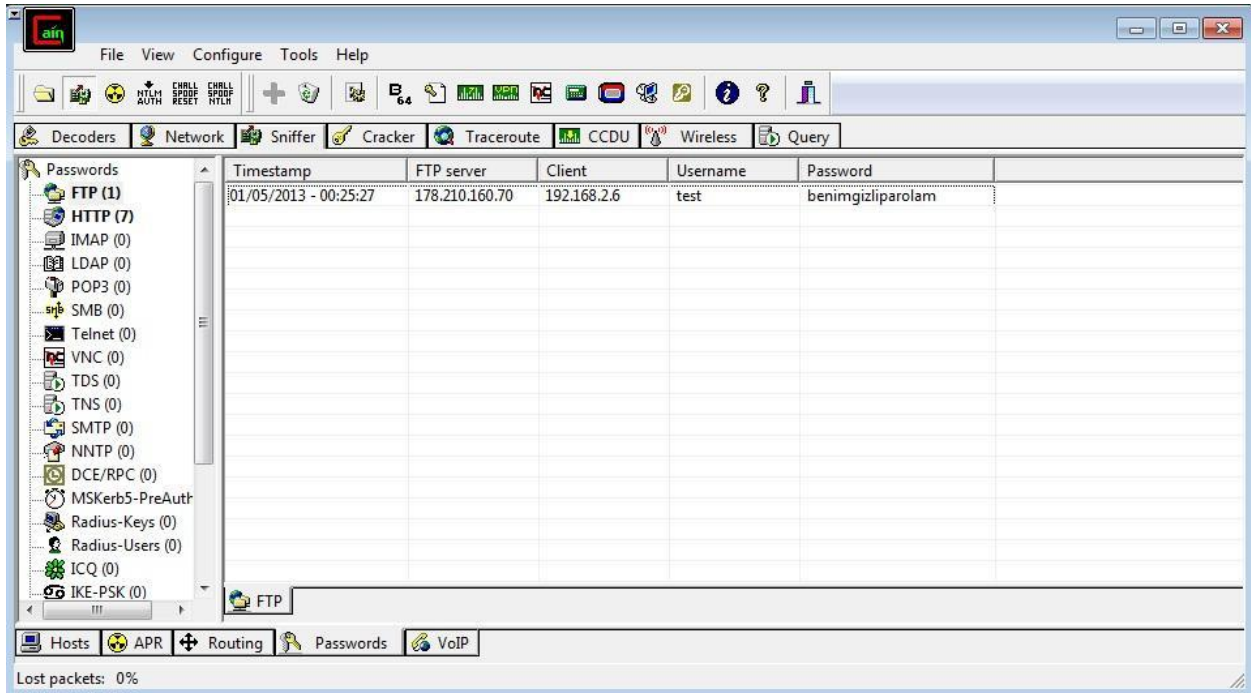
Son durumda bağlantı şekli aşağıdaki gibi devam etmektedir.

```
C:\Windows\system32>arp -a

Interface: 192.168.2.6 --- 0xc
Internet Address      Physical Address      Type
192.168.2.1          00-1a-73-fb-09-8a    dynamic
```



- Cain&Abel uygulamasındaki loglar aşağıdaki gibi olacaktır. FTP,SMTP,HTTP gibi önemli servislerin trafiğini pars ederek daha anlaşılır çıktılar sunacaktır.





### 3.3. DHCP Spoofing Ve DHCP Resource Starvation Denemeleri

**Amaç:** Yerel ağda bulunan bir DHCP sunucusunun IP havuzu tüketilerek, sunucuyu DHCP isteklerine cevap veremez hale getirmek. Sonrasında DHCP sunucu gibi davranarak kurbanlara IP dağıtmak.

**Kullanılan Araçlar:** pig.py, ettercap

**Uygulama:**

- 1. Adım:** Uygulamada önce ağdaki DHCP sunucusu tespit edilecek ve tüm havuzu tüketilecektir.

DHCP havuzunu tüketmek için **pig.py** python betiği kullanılacaktır. Bu betik kali Linux ile birlikte gelmektedir. Kullanım şekli;

```
root@kali:~# pig.py eth0
```

**eth0**; ağ arayüzü olarak girilmektedir.

Betik çalıştırıldığında elde edilen sonuç;

```
root@kali:~# pig.py eth0
WARNING: No route found for IPv6 destination :: (no default route?)

Sending DHCPDISCOVER on eth0
DHCPOFFER handing out IP: 2.2.2.50
sent DHCP Request for 2.2.2.50
waiting for first DHCP Server response on eth0
...
...
...
Sending DHCPDISCOVER on eth0
DHCPOFFER handing out IP: 2.2.2.90
sent DHCP Request for 2.2.2.90

Sending DHCPDISCOVER on eth0
...
```

Havuz tükendiğinde betiğin istekleri cevapsız kalacaktır.

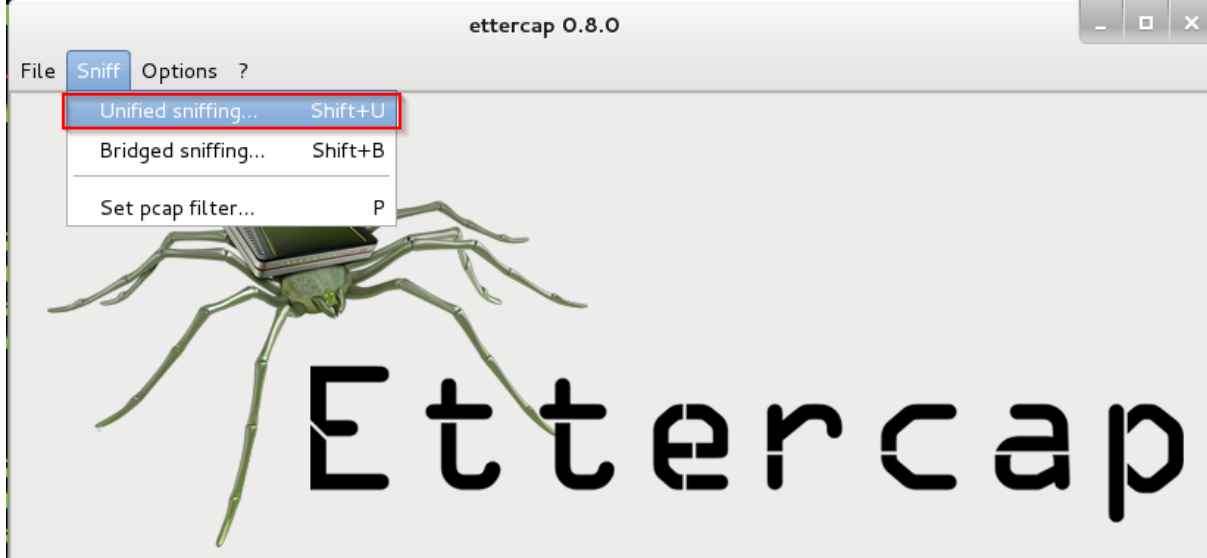
- 2. Adım:** DHCP sunucusu gibi davranarak başkalarının trafiğini üzerinden geçirmek;

Komut satırından ettercap çağrılır;

```
root@kali:~# ettercap -G
```

## [PENTEST LAB ÇALIŞMALARI]

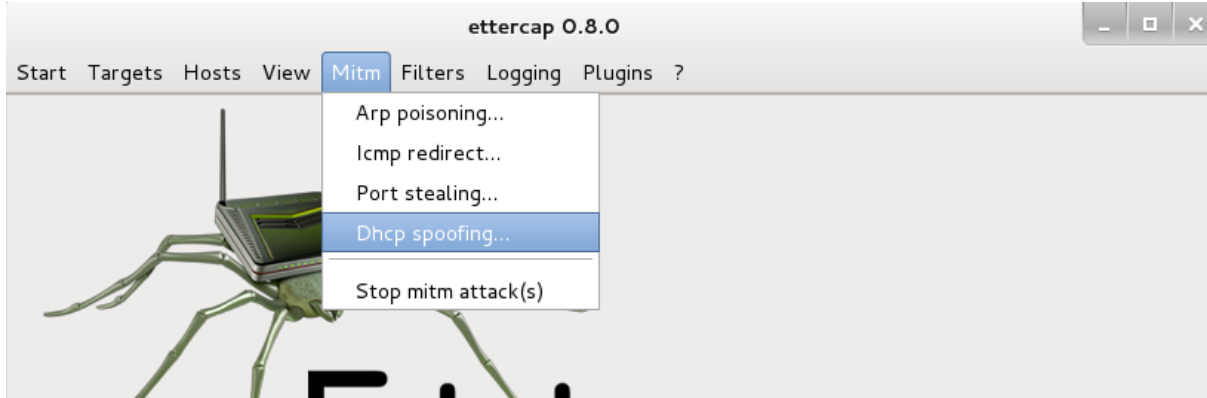
Gelen arayüzden aşağıda işaretlenmiş alan seçilir;



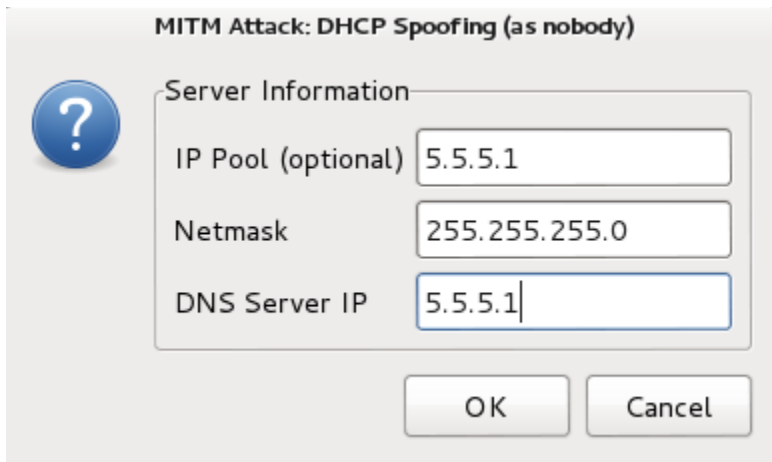
Saldırıda kullanılacak ağ arayüzü seçilir.

**Start -> Start sniffing.** alanı seçilir.

Yeni düzenlenecek menüden **Mitm -> Dhcp spoofing..** seçilir



Saldırıda kullanılacak alanlar doldurulur;



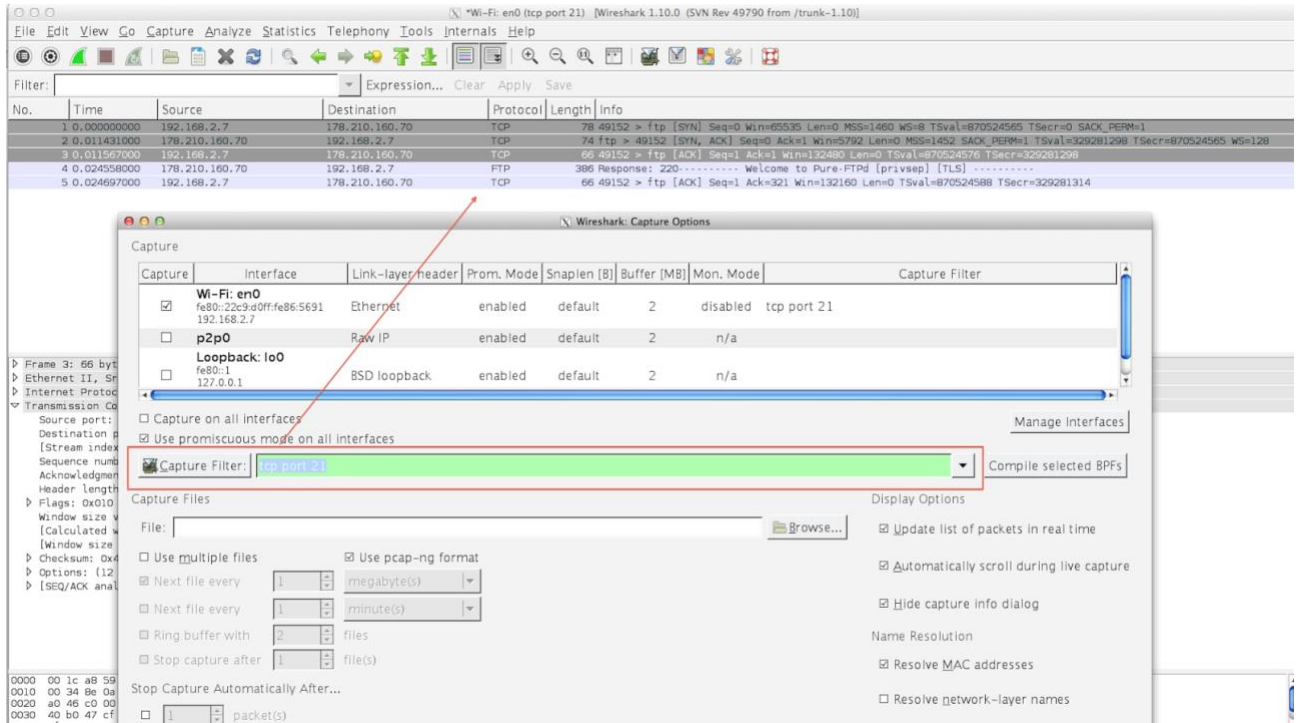
## [PENTEST LAB ÇALIŞMALARI]

### 3.4. Paket/Protokol Analizi Amaçlı Wireshark Kullanımı

**Amaç:** Paket protokol analizinde wireshark aracının kullanılması ve çıktılarının detaylı incelenmesi

Wireshark eski adı Ethereal olan açık kaynak kodlu bir sniffer araçtır. İki tip filtre bulunur.

**Capture Filter :** Yakalanacak paketlerin türü portu protokol bilgisi önceden belirtilerek hedef odaklı bir paket analizi yapılabilir.



**Display Filter :** Yakalanan paketlerin içerisinde istenilen özelliklerdeki paketlerin ayıklanması kısmında kullanılabilir.

# [PENTEST LAB ÇALIŞMALARI]

The image shows a Wireshark capture of network traffic. The filter bar at the top is set to `tcp.srcport == 80`. The packet list pane shows a series of HTTP packets. The packet details pane is expanded to show the Hypertext Transfer Protocol section, indicating it's a continuation of a previous packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
2	0.003427000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
4	0.005600000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
6	0.007184000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
7	0.010307000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
9	0.013522000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
11	0.014929000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
13	0.027134000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
14	0.028909000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
16	0.030938000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
18	0.032596000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
19	0.034151000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
21	0.036995000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
23	0.040135000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
24	0.041737000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic
26	0.053536000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation of non-HTTP traffic

## Adım 1: İzlenen trafik içerisinde kelime arama

The image shows a Wireshark capture of network traffic. The filter bar is set to `dns.qry.name`. The packet list pane shows a series of DNS queries. The packet details pane is expanded to show the Domain Name System (Query) section. A search window is open, showing the search term `berbergokmen` and the search results in the packet bytes pane.

No.	Time	Source	Destination	Protocol	Length	Info
257	4.504274000	192.168.2.7	173.194.39.206	TLSv1	107	Encrypted Handshake Message
258	4.504451000	192.168.2.7	173.194.39.206	TLSv1	1203	Application Data
259	4.537153000	173.194.39.206	192.168.2.7	TCP	66	https > 49714 [ACK] Seq=134 Ack=226 Win=42368 Len=0 TSval=1573130431 TSecr=871760693
260	4.590256000	173.194.39.206	192.168.2.7	TCP	66	https > 49714 [ACK] Seq=134 Ack=1363 Win=42304 Len=0 TSval=1573130485 TSecr=871760693
261	4.606680000	173.194.39.206	192.168.2.7	TLSv1	505	Application Data
262	4.607560000	192.168.2.7	173.194.39.206	TCP	66	49714 > https [ACK] Seq=1363 Ack=573 Win=131296 Len=0 TSval=871760794 TSecr=1573130500
263	4.870551000	Apple_86:56:91	Broadcast	ARP	42	who has 6.6.6.254? Tell 6.6.6.113
264	4.893192000	192.168.2.7	192.168.2.7	DNS	70	Standard query query 0xa2a2.berbergokmen.com
265	5.005944000	8.8.8.8	192.168.2.7	DNS	62	Standard query response 0xa2a2.178.210.160.70
266	5.006572000	192.168.2.7	178.210.160.70	DNS	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
267	5.016842000	178.210.160.70	192.168.2.7	TCP	66	871761191 > 871761191 [ACK] Seq=1 Win=5792 Len=0 MSS=1452 SACK_PERM=1 TSval=330622713 TSecr=871761191 WS=128
268	5.017051000	192.168.2.7	178.210.160.70	TCP	66	871761191 > 871761191 [ACK] Seq=1 Win=132480 Len=0 TSval=871761201 TSecr=330622713
269	5.019271000	192.168.2.7	178.210.160.70	TCP	66	871761191 > 871761191 [ACK] Seq=1 Win=6912 Len=0 TSval=330622734 TSecr=871761203
270	5.037164000	178.210.160.70	192.168.2.7	TCP	66	871761191 > 871761191 [ACK] Seq=1 Win=6912 Len=0 TSval=330622734 TSecr=871761203
271	5.062309000	178.210.160.70	192.168.2.7	TCP	66	871761191 > 871761191 [ACK] Seq=1 Win=6912 Len=0 TSval=330622734 TSecr=871761203

## [PENTEST LAB ÇALIŞMALARI]

**Adım 2:** Protokol detaylarının gösterilmesi, detaylı bir şekilde protokol detayları gösterilir. Özellikle DDOS saldırılarında saldırı tipini belirlemek için kullanılır.

The image shows a Wireshark capture of network traffic. The main window displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A red box highlights the 'Protocol Hierarchy Statistics' window, which provides a detailed breakdown of the traffic by protocol. The statistics are as follows:

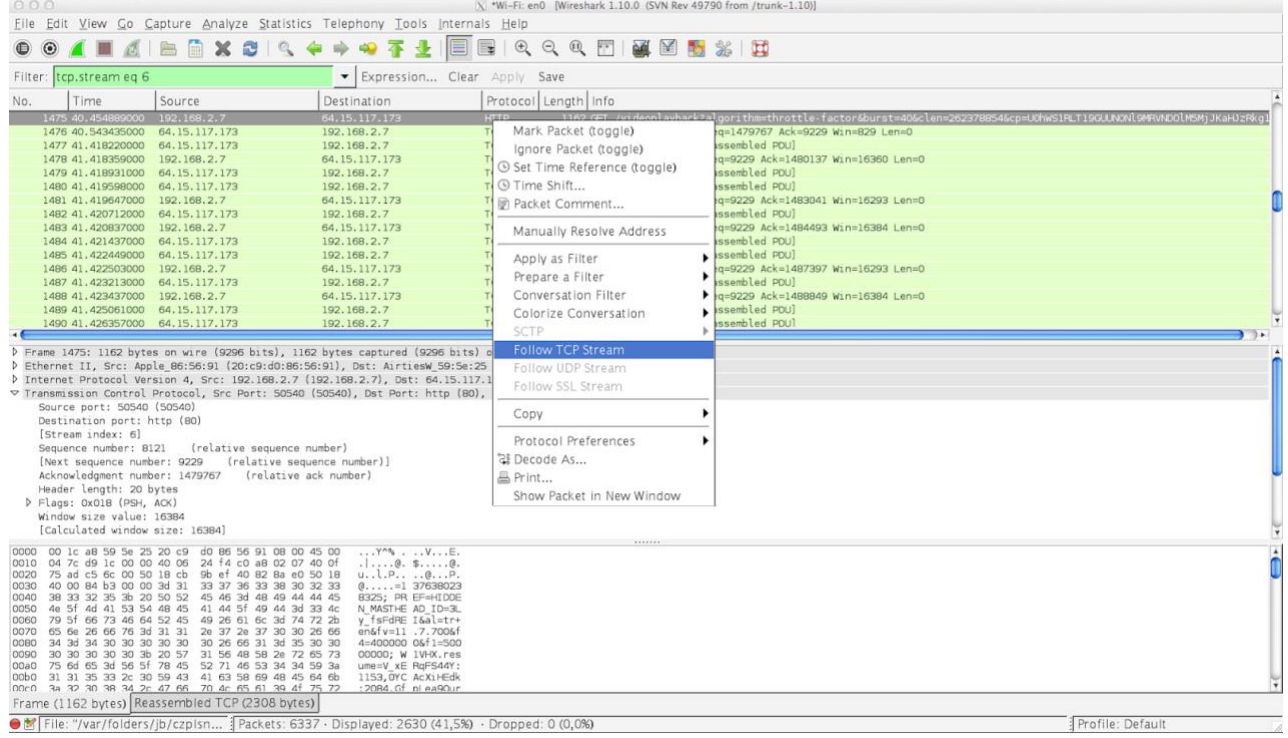
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Ethernet	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Internet Protocol Version 4	99,07 %	6278	99,36 %	6154583	0,435	0	0	0,000
User Datagram Protocol	1,01 %	64	0,12 %	7296	0,001	0	0	0,000
Domain Name Service	0,98 %	62	0,11 %	6730	0,000	62	6730	0,000
Hypertext Transfer Protocol	0,03 %	2	0,01 %	566	0,000	2	566	0,000
Transmission Control Protocol	98,04 %	6213	99,84 %	6147217	0,435	6021	6068695	0,429
Secure Sockets Layer	2,30 %	146	0,70 %	42941	0,003	144	41111	0,003
Secure Sockets Layer	0,03 %	2	0,03 %	1830	0,000	2	1830	0,000
Hypertext Transfer Protocol	0,66 %	42	0,50 %	30937	0,002	24	18724	0,001
Media Type	0,27 %	17	0,18 %	11353	0,001	17	11353	0,001
Line-based text data	0,02 %	1	0,01 %	860	0,000	1	860	0,000
Malformed Packet	0,06 %	4	0,08 %	4644	0,000	4	4644	0,000
Internet Control Message Protocol	0,02 %	1	0,00 %	70	0,000	1	70	0,000
Address Resolution Protocol	0,93 %	59	0,04 %	2478	0,000	59	2478	0,000

The main window also shows a list of packets, with the selected packet (No. 11) being a DNS response from 192.168.2.7 to 173.194.70.1. The packet details pane shows the transaction ID, flags, and the response data.

## [PENTEST LAB ÇALIŞMALARI]

**Adım 3:** TCP oturumlarında paket birleştirme, HTTP bağlantısındaki tüm giden gelen paketlerin birleştirilip session hakkında bilgi verilmesi.

Birleştirilmek istenilen protokol paketi üzerinde sağ tıklanır ve “Follow TCP Stream” seçeneği seçilir.



The screenshot shows the Wireshark interface with a filter set to 'tcp.stream eq 6'. A context menu is open over a selected packet, with 'Follow TCP Stream' highlighted. The packet details pane shows the following information:

```
Frame 1475: 1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface 0  
Ethernet II, Src: Apple_08:00:5E:91:20:C9, Dst: AirtiesW_59:56:25:11:00:00  
Internet Protocol Version 4, Src: 192.168.2.7 [192.168.2.7], Dst: 64.15.117.173  
Transmission Control Protocol, Src Port: 50540 (50540), Dst Port: http (80),  
  Source port: 50540 (50540)  
  Destination port: http (80)  
  [Stream index: 6]  
  Sequence number: 8121 (relative sequence number)  
  [Next sequence number: 9229 (relative sequence number)]  
  Acknowledgment number: 1479767 (relative ack number)  
  Header length: 20 bytes  
  Flags: 0x01B (PSH, ACK)  
  Window size value: 16384  
  [Calculated window size: 16384]
```

The packet bytes pane shows the following hex and ASCII data:

```
0000 00 1c a8 59 5e 25 20 c9 d0 86 56 91 08 00 45 00 ...Y%...V...E.  
0010 04 7c d9 1c 00 00 40 06 24 f4 c0 a8 02 07 40 0f .l...@.$...@.  
0020 75 ad c5 6c 00 50 18 cb 98 ef 40 82 8a e0 50 18 U...lP...@...P.  
0030 40 00 84 b3 00 00 3d 31 33 37 36 33 38 30 32 33 @.....=1 37638023  
0040 38 33 32 35 36 20 50 52 45 46 3d 48 49 44 44 45 8325; PR EF=HEDDE  
0050 46 5f 4d 41 53 54 48 45 41 44 5f 49 44 3d 33 4c N_MASTE HE AD_ID=3L  
0060 79 5f 66 73 46 64 52 45 49 26 61 6c 3d 74 72 2b Y_FASPRE fAal+tr  
0070 65 6e 26 66 76 3d 31 31 2e 37 2e 37 30 30 26 66 eñsfv=11 .7.7006f  
0080 34 3d 34 30 30 30 30 30 26 66 31 3d 35 30 30 4=400000 0mf1=500  
0090 30 30 30 30 30 20 57 31 56 48 58 2e 72 65 73 00000; W lWk; rns  
00a0 75 6d 65 3d 56 5f 78 45 52 71 46 53 34 34 59 3a ume=V_xE RqFS44Y:  
00b0 31 31 35 33 2c 30 59 43 41 63 58 69 48 45 64 6b 1153,0YC AcXlHEdk  
00c0 34 32 30 38 34 2e 47 66 70 4e 6c 61 38 4f 75 72 :20R6 cf ni aa90ur
```

Birleştirilen paketin detayları aşağıda görüldüğü gibi olacaktır. HTTP içerisinden taşınan veri bilgisi.

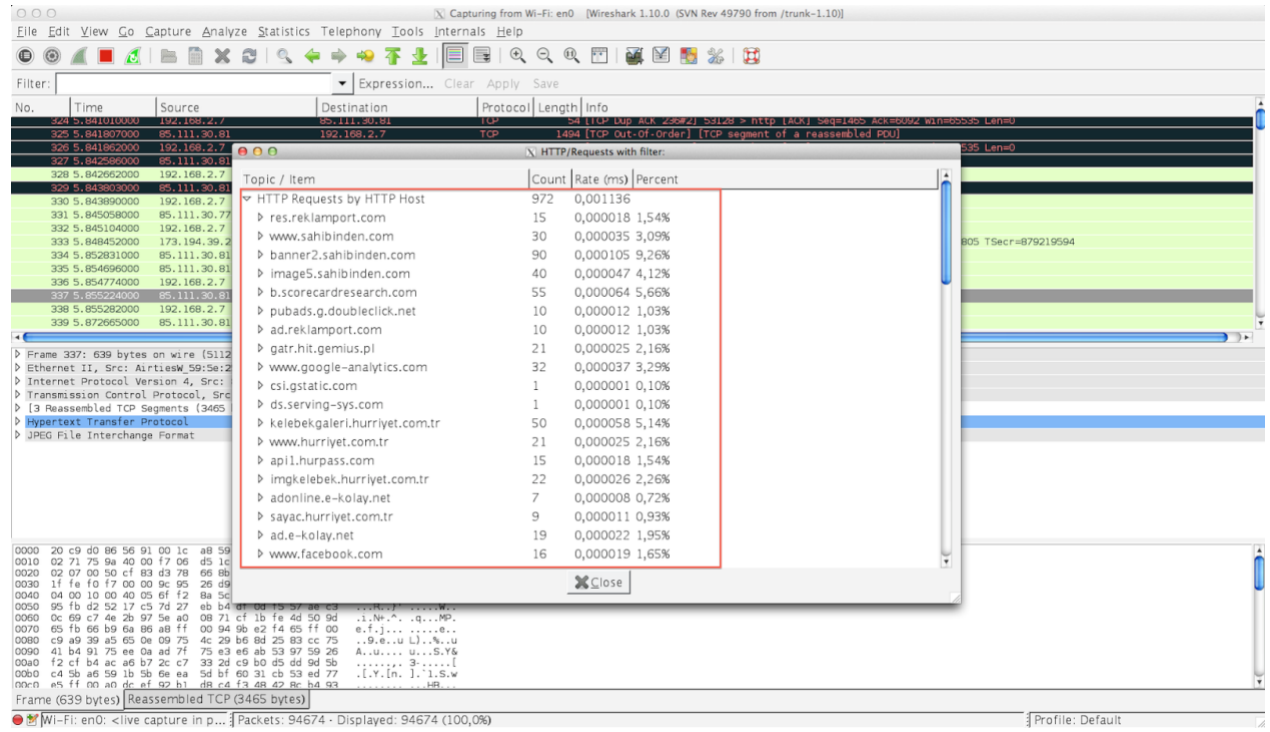
# [PENTEST LAB ÇALIŞMALARI]

The screenshot displays the Wireshark interface with a network capture of a GET request. The main pane shows a list of packets, with packet 1475 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. A 'Stream Content' window is open, showing the raw bytes of the request body, which is a long string of base64-encoded data. The packet list shows a sequence of frames starting from 1475. The packet details pane shows the request structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.



## [PENTEST LAB ÇALIŞMALARI]

### Adım 4: En fazla yapılan HTTP isteğinin gösterilmesi



The screenshot shows the Wireshark interface with a packet capture of an HTTP flood attack. The main pane displays a list of captured packets, with the selected packet (No. 329) being an HTTP GET request to res.reklamport.com. The 'Statistics' pane is open, showing the 'HTTP Requests by Host' table, which is highlighted with a red box. This table lists the top 20 hosts by request count and rate.

Topic / Item	Count	Rate (ms)	Percent
HTTP Requests by HTTP Host	972	0,001136	
▸ res.reklamport.com	15	0,000018	1,54%
▸ www.sahibinden.com	30	0,000035	3,09%
▸ banner2.sahibinden.com	90	0,000105	9,26%
▸ image5.sahibinden.com	40	0,000047	4,12%
▸ b.scorecardresearch.com	55	0,000064	5,66%
▸ pubads.g.doubleclick.net	10	0,000012	1,03%
▸ ad.reklamport.com	10	0,000012	1,03%
▸ gatr.hit.gemius.pl	21	0,000025	2,16%
▸ www.google-analytics.com	32	0,000037	3,29%
▸ csi.gstatic.com	1	0,000001	0,10%
▸ ds.serving-sys.com	1	0,000001	0,10%
▸ kelebekgaleri.hurriyet.com.tr	50	0,000058	5,14%
▸ www.hurriyet.com.tr	21	0,000025	2,16%
▸ api1.hurpass.com	15	0,000018	1,54%
▸ imgkelebek.hurriyet.com.tr	22	0,000026	2,26%
▸ adonline.e-kolay.net	7	0,000008	0,72%
▸ sayac.hurriyet.com.tr	9	0,000011	0,93%
▸ ad.e-kolay.net	19	0,000022	1,95%
▸ www.facebook.com	16	0,000019	1,65%

DDOS saldırı (HTTP Flood) tipi analizinde oldukça yararlı bir özellik olarak kullanılabilir.

### 3.5. Network Miner İle Trafik Analizi

**Amaç:** NetworkMiner aracını kullanarak kaydedilmiş bir trafiği incelemek

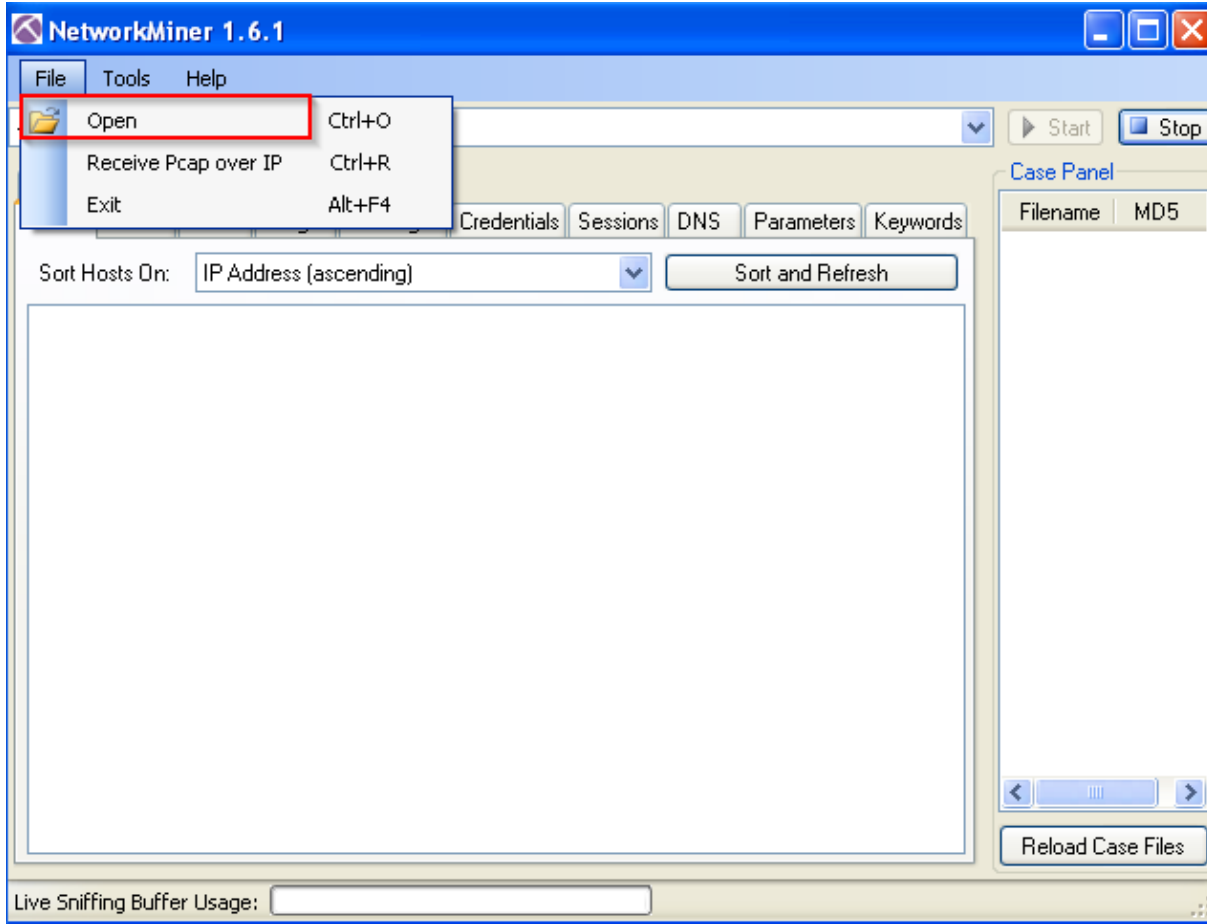
**Kullanılan Araçlar:** NetworkMiner

**Uygulama:** Yerel ağdan elde edilen trafik networkminer aracı ile analiz edilip, yerel ağda gerçekleştirilen işlemler anlamlandırılmaya çalışılacaktır.

Networkminer aracının ücretsiz ve ticari sürümleri bulunmaktadır, burada ücretsiz sürümü üzerinden program tanıtılacaktır.

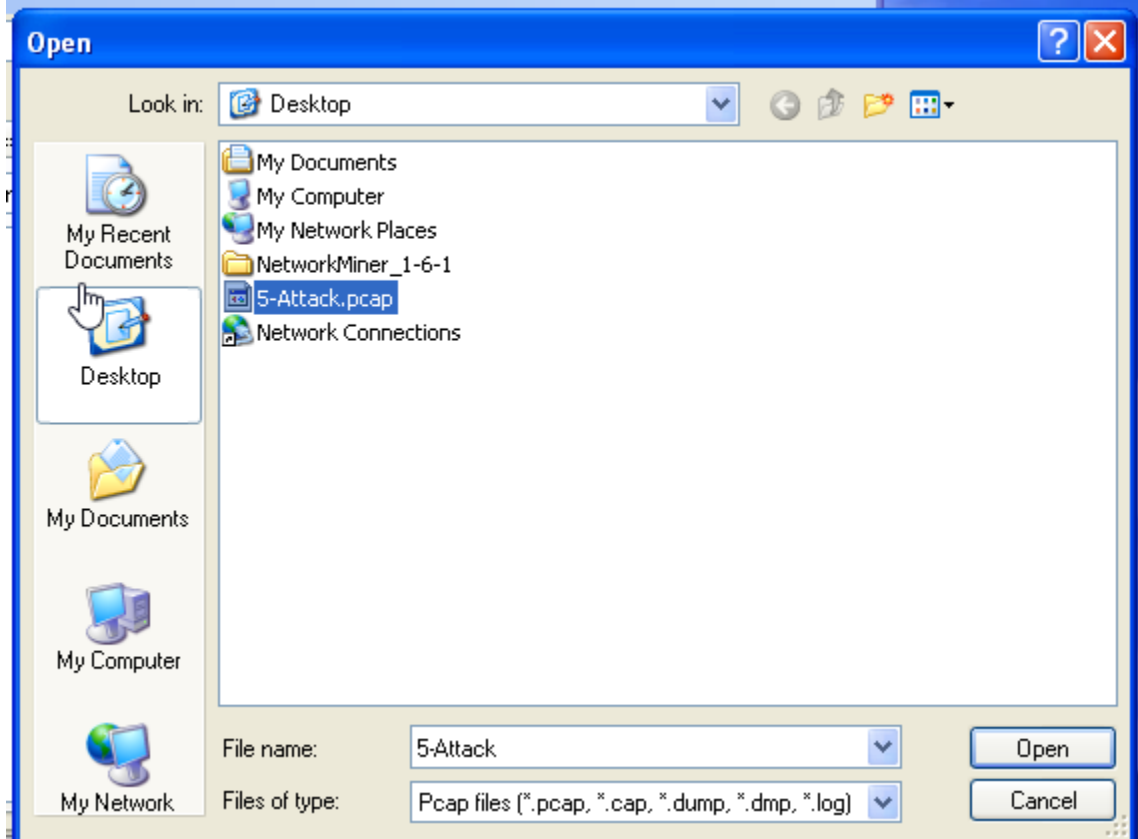
Networkminer aracı <http://sourceforge.net/projects/networkminer/> adresinden indirmek mümkün. Araç herhangi bir kurulum gerektirmemektedir. Çalıştırılması yeterlidir.

Yeni bir paketin incelenmek üzere tanıtılması için, aşağıda gösterildiği gibi File → Open seçenekleri seçilir.



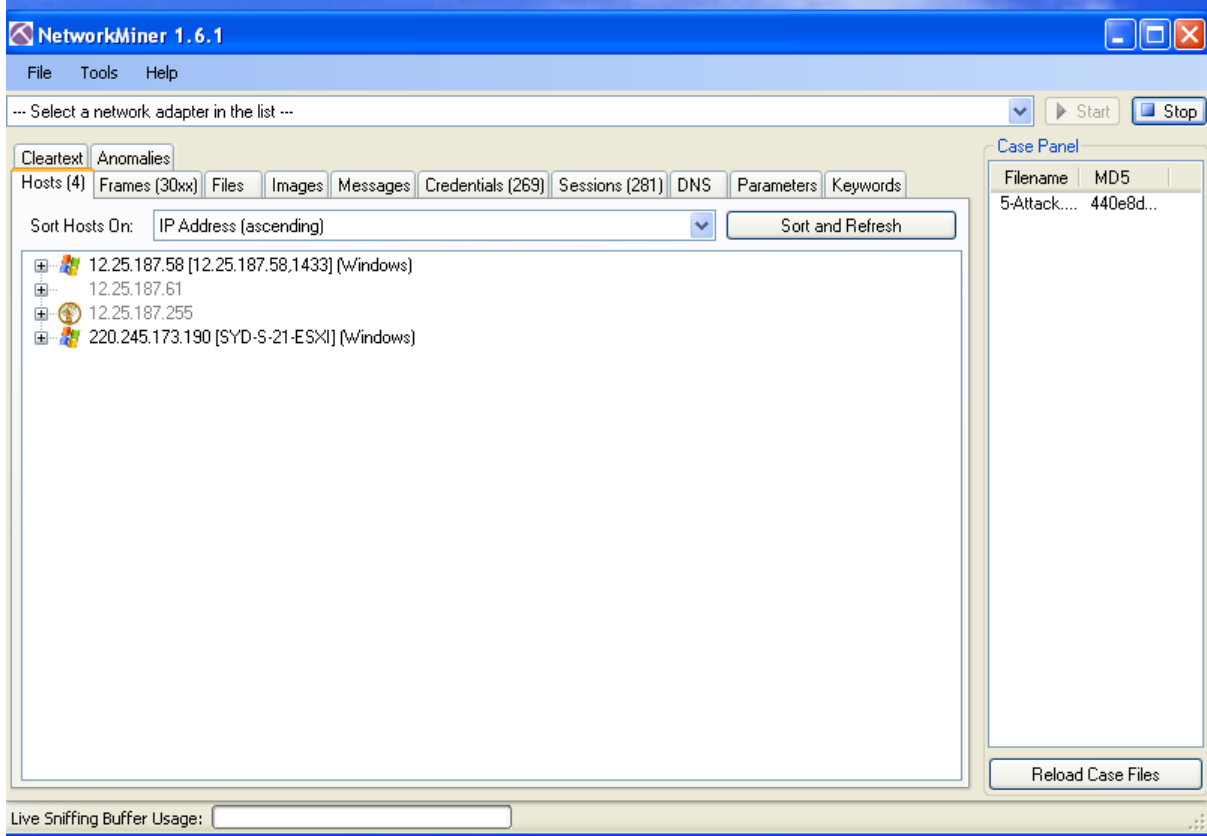
## [PENTEST LAB ÇALIŞMALARI]

Hedef pcap dosyasının tanıtılma işlemi:



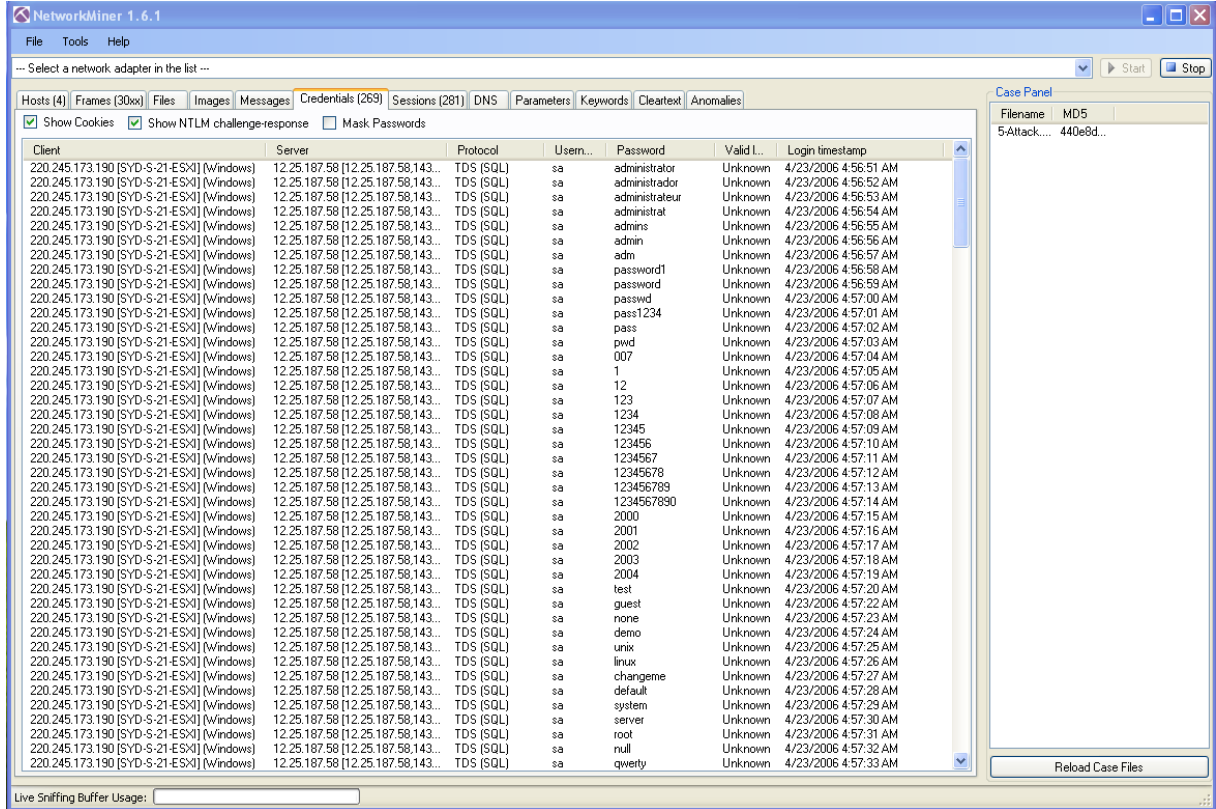
Araca trafiğin kayıt dosyası eklenince, bir analiz işlemi gerçekleştirilecektir.

## [PENTEST LAB ÇALIŞMALARI]



Burada görüldüğü üzere bazı alanlarda tespitler yapılmıştır. Burada “Credential” sekmesine bakıldığında:

## [PENTEST LAB ÇALIŞMALARI]



The screenshot displays the NetworkMiner 1.6.1 application window. The main area shows a list of credentials with columns for Client, Server, Protocol, User, Password, Valid L., and Login timestamp. The Case Panel on the right shows the filename 'MD5' and a list of files including '5Attack...' and '440e8d...'. The interface includes a menu bar (File, Tools, Help) and a toolbar with 'Start' and 'Stop' buttons. The main window title is 'NetworkMiner 1.6.1'.

Client	Server	Protocol	User...	Password	Valid L.	Login timestamp
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	administrator	Unknown	4/23/2006 4:56:51 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	administrador	Unknown	4/23/2006 4:56:52 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	administrateur	Unknown	4/23/2006 4:56:53 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	administrat	Unknown	4/23/2006 4:56:54 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	admins	Unknown	4/23/2006 4:56:55 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	admin	Unknown	4/23/2006 4:56:56 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	adm	Unknown	4/23/2006 4:56:57 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	password1	Unknown	4/23/2006 4:56:58 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	password	Unknown	4/23/2006 4:56:59 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	passwd	Unknown	4/23/2006 4:57:00 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	pass1234	Unknown	4/23/2006 4:57:01 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	pass	Unknown	4/23/2006 4:57:02 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	pwd	Unknown	4/23/2006 4:57:03 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	007	Unknown	4/23/2006 4:57:04 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	1	Unknown	4/23/2006 4:57:05 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	12	Unknown	4/23/2006 4:57:06 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	123	Unknown	4/23/2006 4:57:07 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	1234	Unknown	4/23/2006 4:57:08 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	12345	Unknown	4/23/2006 4:57:09 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	123456	Unknown	4/23/2006 4:57:10 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	1234567	Unknown	4/23/2006 4:57:11 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	12345678	Unknown	4/23/2006 4:57:12 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	123456789	Unknown	4/23/2006 4:57:13 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	1234567890	Unknown	4/23/2006 4:57:14 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	2000	Unknown	4/23/2006 4:57:15 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	2001	Unknown	4/23/2006 4:57:16 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	2002	Unknown	4/23/2006 4:57:17 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	2003	Unknown	4/23/2006 4:57:18 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	2004	Unknown	4/23/2006 4:57:19 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	test	Unknown	4/23/2006 4:57:20 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	guest	Unknown	4/23/2006 4:57:22 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	none	Unknown	4/23/2006 4:57:23 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	demo	Unknown	4/23/2006 4:57:24 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	unix	Unknown	4/23/2006 4:57:25 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	linux	Unknown	4/23/2006 4:57:26 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	changeme	Unknown	4/23/2006 4:57:27 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	default	Unknown	4/23/2006 4:57:28 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	system	Unknown	4/23/2006 4:57:29 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	server	Unknown	4/23/2006 4:57:30 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	root	Unknown	4/23/2006 4:57:31 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	null	Unknown	4/23/2006 4:57:32 AM
220.245.173.190 [SYD-S-21-ESXII] [Windows]	12.25.187.58 [12.25.187.58,143...]	TDS (SQL)	sa	qwerty	Unknown	4/23/2006 4:57:33 AM

Hedef sistemin bir veritabanı sunucusu olduğu ve saldırganın bu sisteme giriş denemelerinde bulunduğu görülmektedir.

Not: Bu doküman BGA Bilgi Güvenliği A.Ş için Mesut Türk tarafından hazırlanmıştır.