ARP Protokolü ve Güvenlik Zafiyeti

@2014

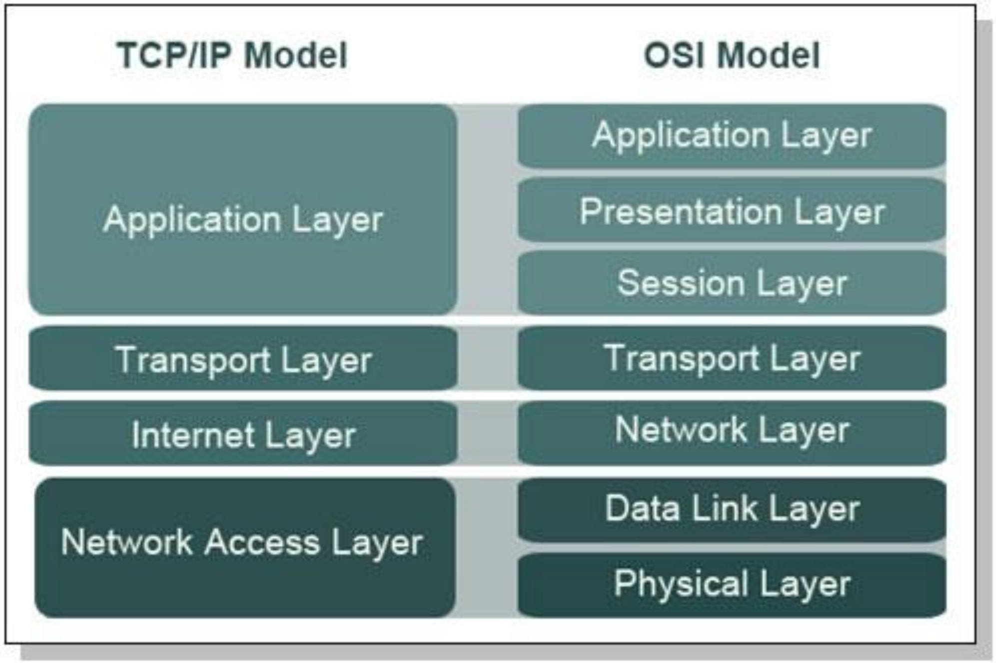
Örnek Eğitim Notu

bilgi@bga.com.tr

ARP Protokolü ve Güvenlik Zafiyetleri

L2 Katmanı

- OSI 2. Katman: Data Link Layer
- 2. Katman Protokolleri
  - ATM, CDP, ARP, Frame Relay, Ethernet, IEEE 802.11, PPP
- TCP/IP : Link Layer



http://learn-networking.com/tcp-ip/the-tcpip-stack-and-the-osi-model

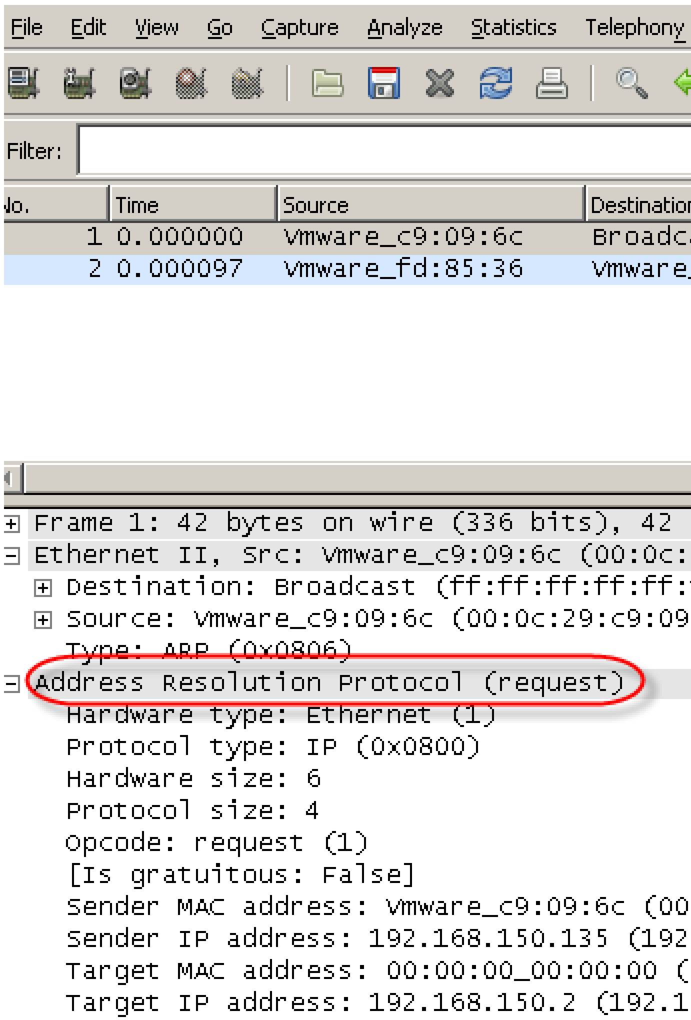
Address Resolution Protocol(ARP)

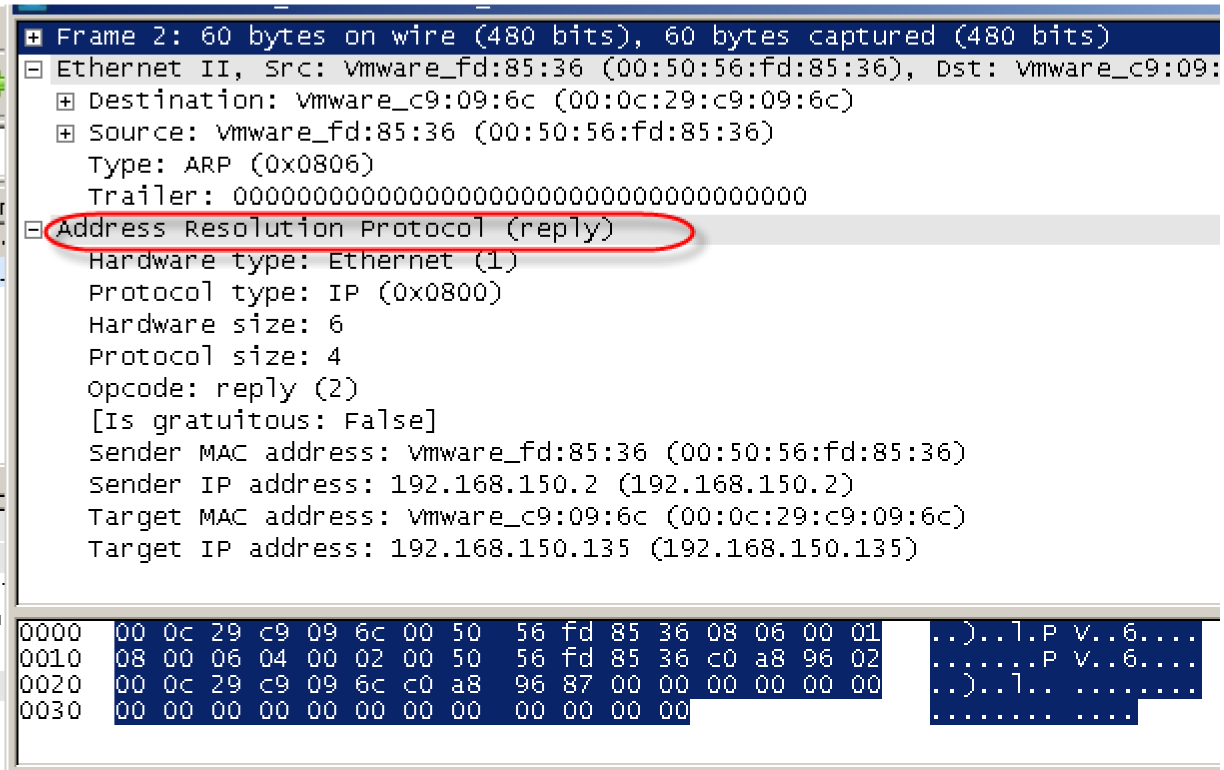
- Yerel ağlarda iki hostun birbiri ile anlaşabilmesi için kullanılan protokoldür.(RFC 826)
- İki host birbiri ile iletişime geçmeden önce birbirlerinin IP adreslerini bilmek zorundadır.
  - IP adresini bilenlerin iletişime geçebilmesi için MAC adreslerini edinme zorunluluğu vardır.
- TCP/IP iletişiminde en önemli(?) protokoldür
- Ipv6 'da ARP yerine benzeri işlevi yerine getiren Neighbor Discovery Protocol (NDP) geliyor.
- ARP iki işlemli bir süreçtir.
  - ARP Request
  - ARP Reply

ARP Başlık Bilgisi

<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware
length</td><td>Protocol
length</td><td>Operation
Request 1, Reply 2</td></tr>
<tr><td colspan="3">Sender hardware address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender protocol address
(For example, 4 bytes for IP)</td></tr>
<tr><td colspan="3">Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled in a request)</td></tr>
<tr><td colspan="3">Target protocol address
(For example, 4 bytes for IP)</td></tr>
</table>

ARP Başlık Bilgisi – Sniffer Çıktısı





ARP Çalışma Mantığı

- Birbirini tanımayan insanların bulunduğu ortamdaki tanışma mantığı ARP'ı en iyi özetleyen durumdur.
- Kimse birbirini tanımadığı için bağırarak aradığı kişinin ismini söyler.
- Aradığı ... lse tekrar s... sonra sormay...

ARP Paket Çeşitleri

- 4 cesit ARP paketi vardır

ARP request : IP Adresine ait donanım adresi(MAC adresi) sorgulamak için kullanılır

10:09:20.356809 arp who-has 12.16.6.17 tell 12.16.6.185

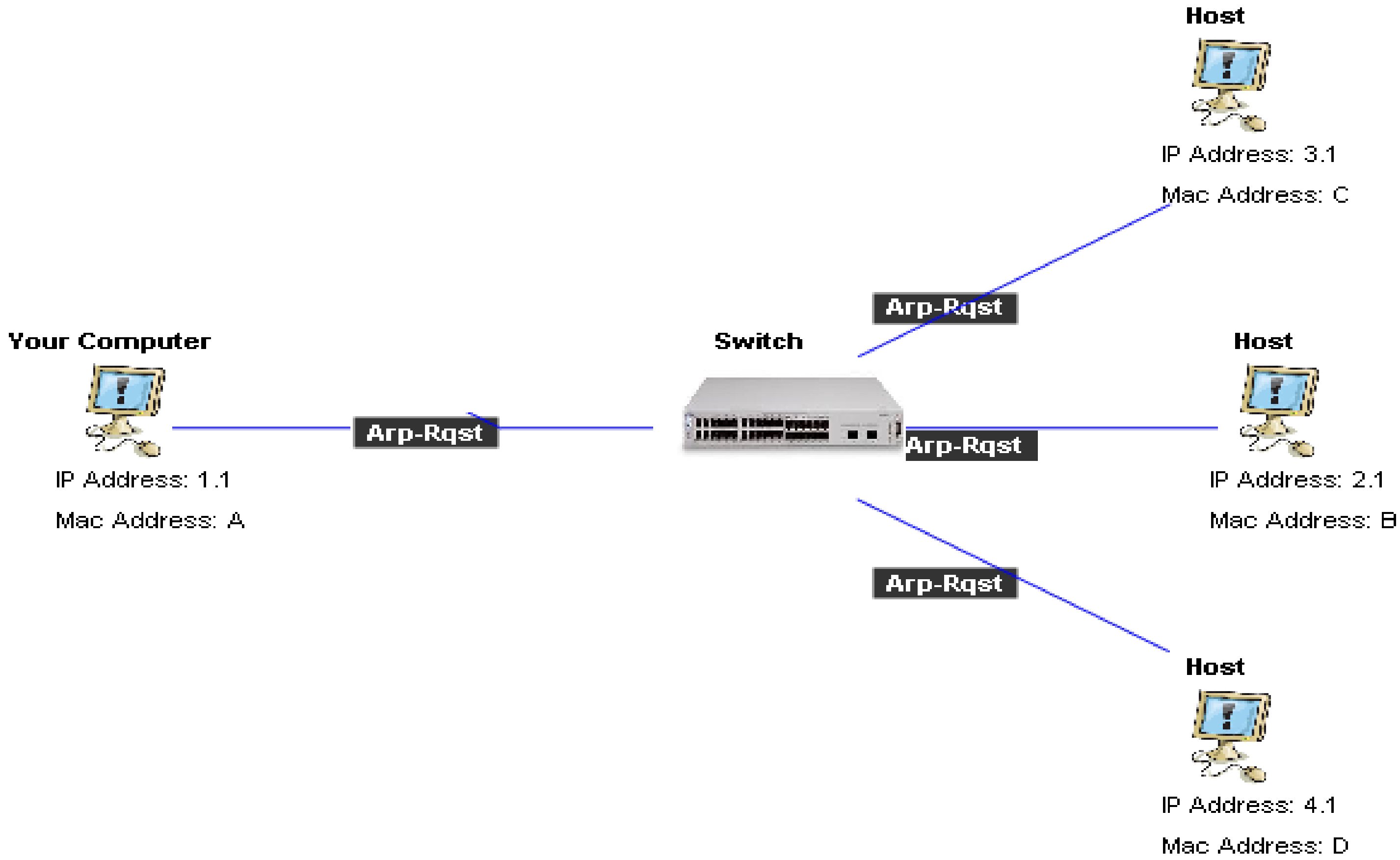
ARP reply : Belirtilen Ip adresine uyan donanım adresini döndürür

10:09:20.356809 arp reply 12.16.6.17 is-at 0:80:c8:f8:5c:73

RARP request: Belirli bir MAC adresi için IP adresi sorgulaması için kullanılır

RARP reply : Belirli MAC adresi için IP adresi cevabı döndürür.

Arp Request



ARP REQUEST(Broadcast)

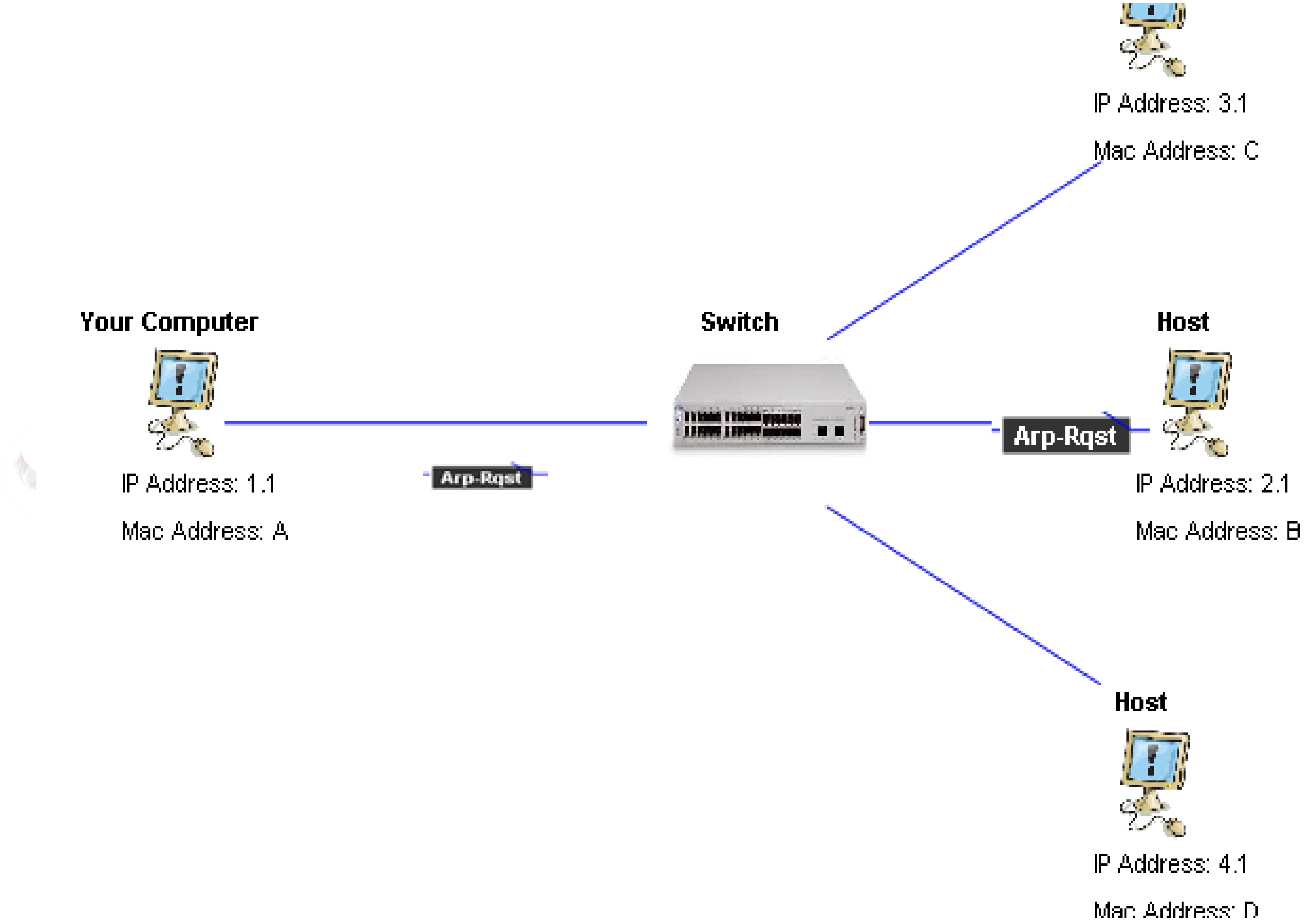
Arp Request(Detay)

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Runtop_e1:59:6e	Broadcast	ARP	Who has 10.234.8.1? Tell 10.234.10.77
2	0.008060	Cisco_3c:3f:a8	Runtop_e1:59:6e	ARP	10.234.8.1 is at 00:01:96:3c:3f:a8

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Runtop_e1:59:6e (00:20:78:e1:59:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Runtop_e1:59:6e (00:20:78:e1:59:6e)
    Sender IP address: 10.234.10.77 (10.234.10.77)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.234.8.1 (10.234.8.1)
```

ARP REQUEST(Broadcast)

Arp Reply



ARP REPLY(Unicast)

Arp Request-Arp Reply (Detay)

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Runtop_e1:59:6e	Broadcast	ARP	Who has 10.234.8.1? Tell 10.234.10.77
2	0.008060	Cisco_3c:3f:a8	Runtop_e1:59:6e	ARP	10.234.8.1 is at 00:01:96:3c:3f:a8

```
⊞ Frame 2 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Cisco_3c:3f:a8 (00:01:96:3c:3f:a8), Dst: Runtop_e1:59:6e (00:20:78:e1:59:6e)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: Cisco_3c:3f:a8 (00:01:96:3c:3f:a8)
    Sender IP address: 10.234.8.1 (10.234.8.1)
    Target MAC address: Runtop_e1:59:6e (00:20:78:e1:59:6e)
    Target IP address: 10.234.10.77 (10.234.10.77)
```

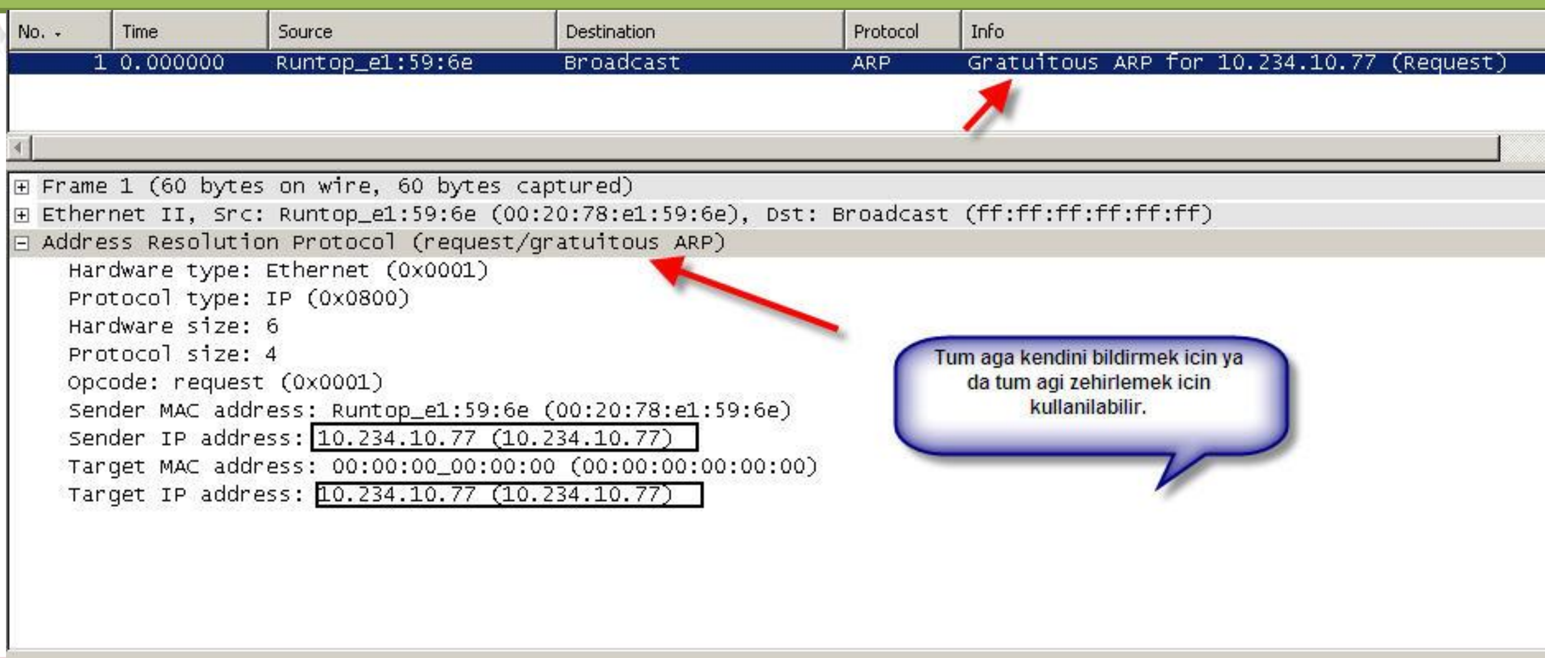
ARP REPLY(Unicast)

Gratious ARP Paketleri

- Ağa bağlanan makinenin tüm ağa kendini tanıtmak için kullandığı ARP paketi tipi.

```
#ifconfig rl0 inet 192.168.15.1
```

17:25:40.216489 **00:50:ba:15:19:0d** > Broadcast, ethertype ARP (0x0806), length 60: **arp who-has 192.168.15.1 tell 192.168.15.1**



Gratious ARP Paketleri HA Firewall

- Gratious ARP paketleri birden fazla güvenlik duvarının failover çalıştığı durumlarda sık kullanılır.
- İki güvenlik duvarı tek bir IP adresini paylaşıyorsa master olan gittiğinde yedekte duran güvenlik duvarının trafiği üzerine alabilmesi ortak IP adresinin MAC adresini kendisi olarak anons etmesiyle mümkündür.
- Bu tip gereksinimlerde Gratious Arp paketleri kullanılır.

Arping

- Arping adından da anlaşılacağı gibi Layer 2 seviyesinde ping atmaya yarayan bir araçtır.
- Arping kullanarak Layer 2 seviyesinde bir makinenin açık olup olmadığı, ağdaki ip çakışmaları, bir ip adresinin ağda kullanılıp kullanılmadığı gibi bilgiler edinilebilir.
- Aynı zamanda arping kullanılarak gratious arp paketleri üretilebilir.
- Gratious paketlerle bir ip adresine ait mac adresi tüm yerel ağdaki sistemlerde güncellenebilir.
- Arping ARP Request ve Reply paketleri kullanır.
- *Not: arping'i diğer l3 ping araçlarından ayıran önemli özelliği ağ arabirimi üzerinde ip adresi olmasa dahi ping işlemlerini gerçekleştirebilir(yani L2 de çalışabilir).*

Temel Arping Kullanımı

- arping'in en basit kullanımı ağdaki bir ip adresinin L2 seviyesinde MAC adresinin alınmasıdır. Bunu aşağıdaki komutla gerçekleyebiliriz.

root@home-labs:**~# arping 192.168.2.1 -c 1**
ARPING 192.168.2.1 from 192.168.2.23 eth0
Unicast reply from 192.168.2.1 [00:1A:2A:A7:22:5C] 1.860ms
Sent 1 probes (1 broadcast(s))
Received 1 response(s)

root@home-labs:**~# tcpdump -i eth1 -tttnn arp**
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
000000 arp who-has 192.168.2.1 (ff:ff:ff:ff:ff:ff) tell 192.168.2.23
000918 arp reply 192.168.2.1 is-at 00:1a:2a:a7:22:5c

Ağdaki IP Çakışmalarının Bulunması

- Ağınızda IP çakışmasından şüpheleniyorsanız arping kullanarak emin olabilirsiniz.

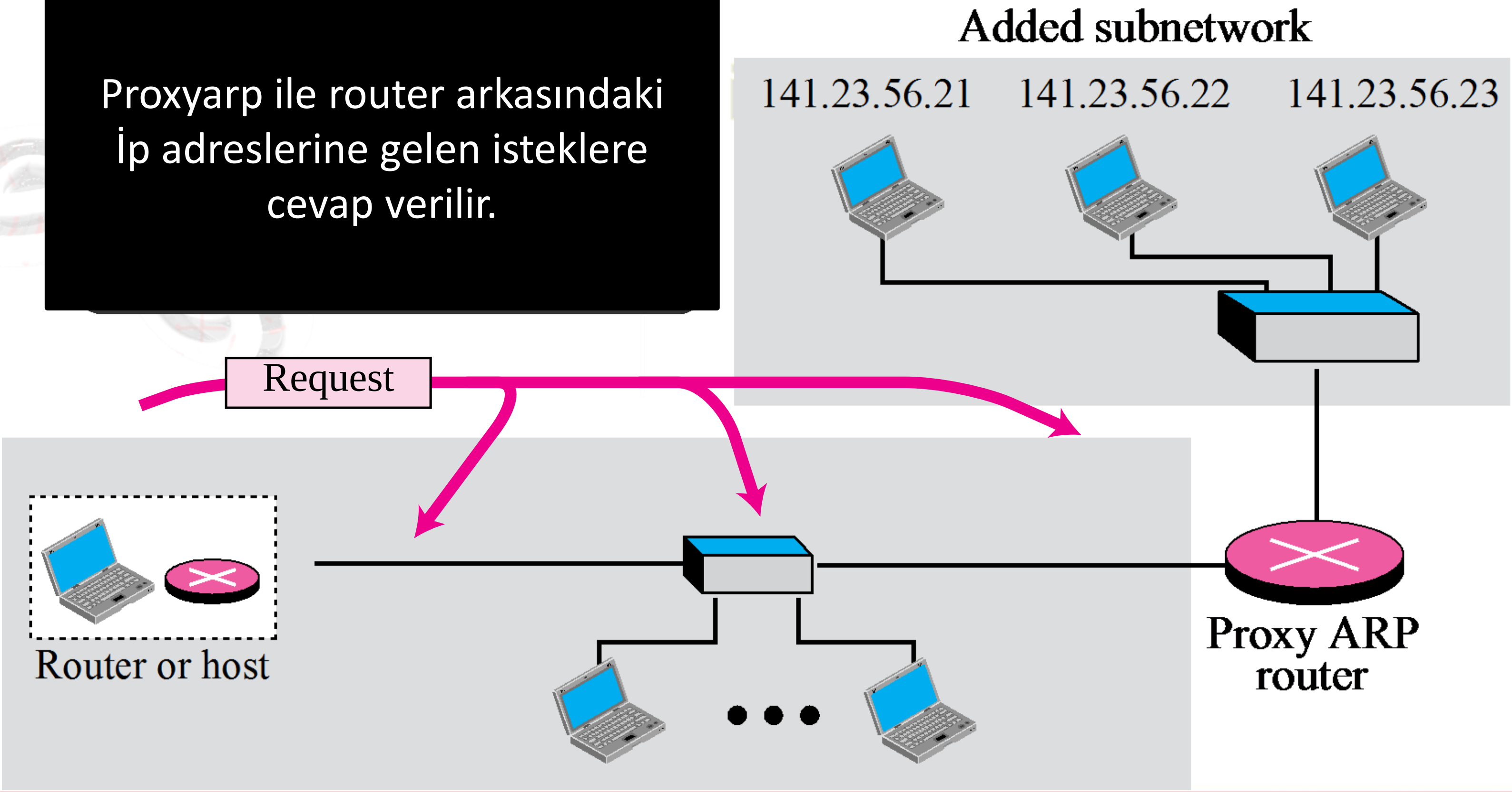
arping -I eth1 -D 192.168.2.20

000000 arp who-has 192.168.2.20 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0
000140 arp reply 192.168.2.20 is-at 00:0c:29:06:df:e4
001738 arp reply 192.168.2.20 is-at 00:1b:77:9b:cb:e2

- Yukarıdaki çıktıda 192.168.2.20 ip adresi için yapılan sorguya iki farklı mac adresi cevap veriyor.
- Bu çıktı ağda IP çakışmasının olduğu manasına gelir.
-

Proxy ARP

Proxyarp ile router arkasındaki İp adreslerine gelen isteklere cevap verilir.

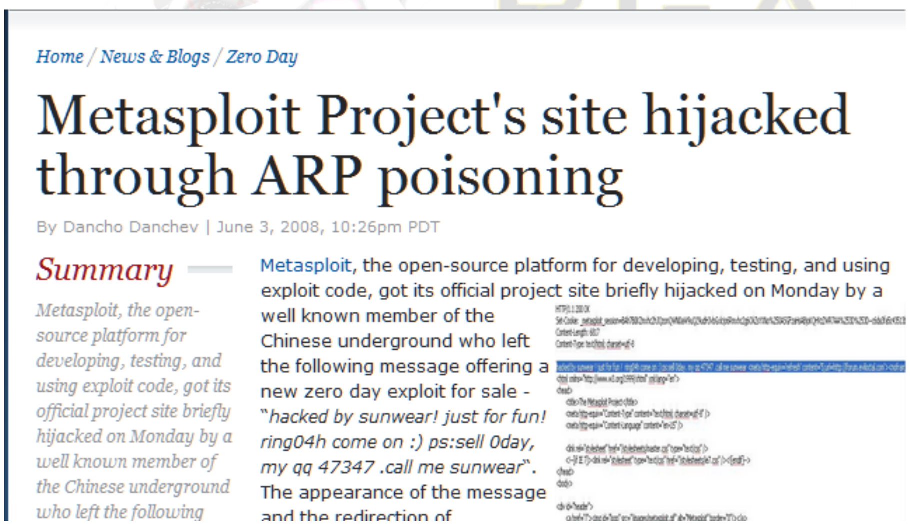


ARP’ın Güvenlik Açısından Önemi

- **ARP,** yerel ağlarda iletişimin başladığı ilk noktadır.
- Protokol doğası herhangi bir koruma/korunma mekanizması yoktur.
- Sunucu sistemlerin bulunduğu ortamlar da birer yerel ağlardır.
  - DMZ, eğer yeteri kadar önlem alınmamışsa kendi içinde LAN’dır.
- Eğer ek güvenlik önlemleri alınmamışsa bir ağda ele geçirilen makine diğer tüm makinelerin güvenliğini tehdit eder!
- MITM saldırıları kullanılarak yerel ağda diğer sistemlerin bilgileri ele geçirilebilir.

Metasploit.com Arp Poisoning

- *"Another customer on the same ISP was compromised and used to ARP poison all servers in that subnet. I corrected the problem by setting a static ARP entry and notifying the ISP. To make it very clear - the metasploit.com servers were not compromised, nor have been to this date,"* he said



Post Exploitation|ARP Cache Poisoning

- ARP cahce poisoning yerel ağ saldırısı olarak gözükse de genellikle birçok saldırıda ara bileşen olarak kullanılır.
- Saldırgan web zaafiyetini kullanarak DMZ'de bir makineyi ele geçirir.
- Diğer makinelere atlamak için kullanacağı en kolay yol ARP spoofing, cache poisoning yöntemini kullanmaktır.
  - Arp spoofing yaparak: ftp, telnet, http, RDP parolalarını ele geçirebilir.
  - İstediği DMZ makinesini internet üzerinden hacklenmiş gösterebilir.(Metasploit.com örneği)

ARP Protokolüne Dayalı L2 Saldırıları

- ARP Spoofing & ARP Poisoning
- ARP DoS
- Mac Flooding
- Kablosuz Ağlarda L2 saldırıları
  - MAC Onaylamalı Ağlara izinsiz girme
  - DOS
  - ARP cache Poisoning
- ARP Spoof sonrası gerçekleştirilebilecek muhtemel saldırılar
  - SSH & SSL bağlantılarda araya girme
  - HTTP bağlantılarında araya girme
  - DNS isteklerini yönlendirme
  - HTTP bağlantılarında cookie çalma.

Kablosuz Ağlarda ARP

- Kablosuz ağlarda istemcinin durumu
  - Managed Mod:Ağa bağlıdır, klasik L2 ortamı
  - Monitor mode: Ağa bağlı değildir, ilgili kanalı izler ve şifrelenmemiş verileri görür
- MAC adresi filtrelemesini aşma
  - Monitor modda trafik dinlenir
  - Yetkili bir mac adresi öğrenilir ve o MAC adresi üzerine alınır.
  - Aynı MAC adresine sahip diğer istemcinin durumu???
- Bağlı Kullanıcılara yanlış ARP kayıtları göndererek DOS'a maruz bırakma

Kablosuz Ağlarda ARP-II

- 802.11 protokolü tamamlandıktan sonra ethernet ağlarda geçerli kurallar kablosuz ağlar için de geçerlidir.
- L2'de geçerli tüm saldırılar (MITM, DoS vs) Wifi için de geçerlidir.
- Şifreleme kullanılması bu tip saldırıları engellemez
  - Parolayı bilip ağa dahil olan istemciler için.
- Kablosuz ağ cihazında Client Isolation gibi bir özellik kullanılıyorsa cihaza bağlı istemciler birbirlerine ait trafiği izleyemez, değiştiremez.

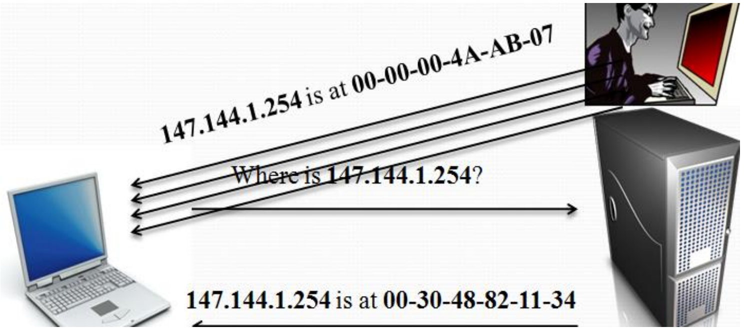
ARP Cache

- İşletim sistemleri erişmek istedikleri ip adreslerine her seferinde ARP sorgusu göndermek yerine aldıkları ARP cevaplarını bir müddet saklarlar.
- Bu saklanan bilgiye ARP kaydı denir.
- Arp kayıtlarını listeleme
  - Arp –a, arp –an komutlarıyla gerçekleştirilir.
- ARP kaydı silme
  - Arp –d 192.168.1.1.

```
C:\Documents and Settings\Administrator>arp -a

Arabirim: 192.168.150.135 --- 0x2
  Internet Adresi         Fiziksel Adres        Tipi
  192.168.150.2           00-50-56-fd-85-36     dinamik

C:\Documents and Settings\Administrator>
```

ARP Cache Poisoning

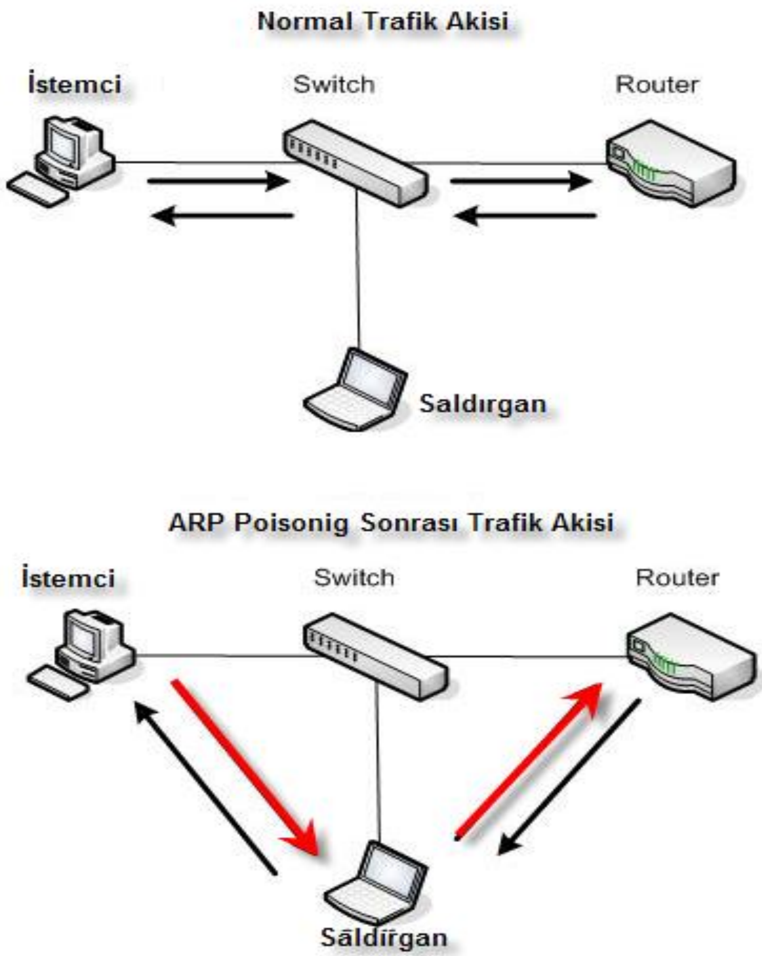
- **Amac:** Hedef sisteme sahte arp paketleri göndererek kendisini farklı bilgisayar gibi (Gateway?) göstermek ve kurbanın göndereceği trafiği üzerinden geçirmektir.
- Poisoning ?
  – Hedef sistemin arp belleğinin zehirlenmesi.
- ARP Spoofing yerel aglarda gerceklestirilebilir.
  – Bunun sebebi de ARP protokolunun L2'de çalışmasıdır.



ARP Poisoning, Spoofing Saldırıları

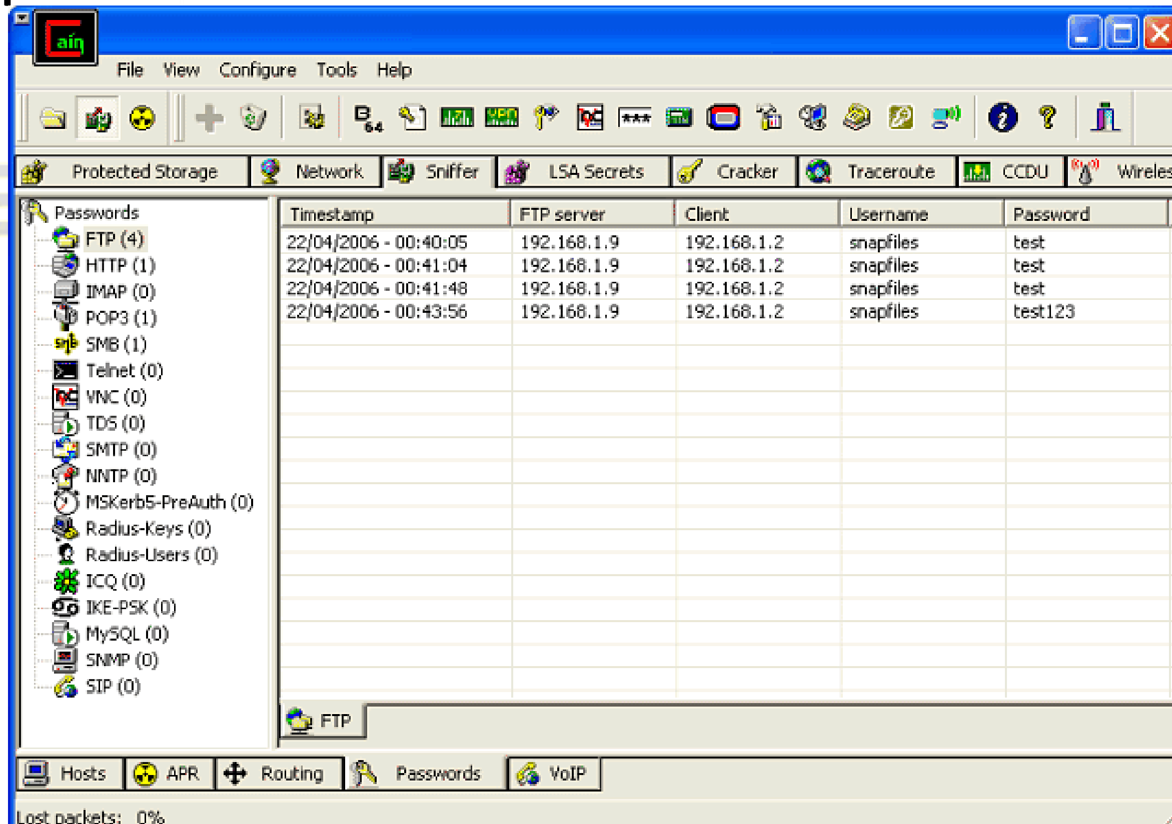
- Yerel ağlarda iletişimin başladığı nokta olan ARP seviyesinde araya girildikten sonra tüm trafik saldırgan üzerinden geçer.
- Saldırgan trafiği başarıyla kendi üzerinden geçirebildiyse;
  - Tüm trafiği okuyabilir
  - Şifreli değilse yrumlayabilir
  - Engelleyebilir
  - Değiştirebilir
- Tüm bu saldırılarda amaç iki farklı nokta haberleşirken araya girip iletişim detaylarını edinme ya da engellemedir.

ARP Cache Poisoning-II



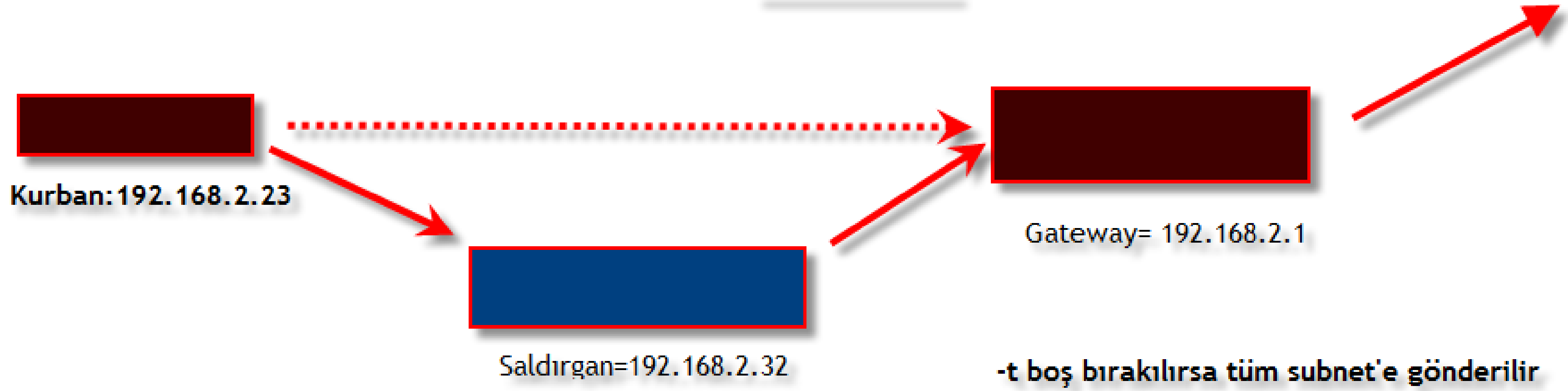
ARP Saldırı Araçları

- Windows ve Linux için çeşitli araçlar bulunmaktadır
- Windows araçları
  - Winarpspoof
  - Ettercap
  - Cain&Abel
- Linux Araçları
  - Arpspoof
  - Ettercap
  - Nemesis
  - Scapy



Arpspoof Yazılımı

```
root@guvenlikod: /home/huzeyfe
root@guvenlikod:/home/huzeyfe#
root@guvenlikod:/home/huzeyfe# arpspoof -i eth0 -t 192.168.2.23 192.168.2.1
```

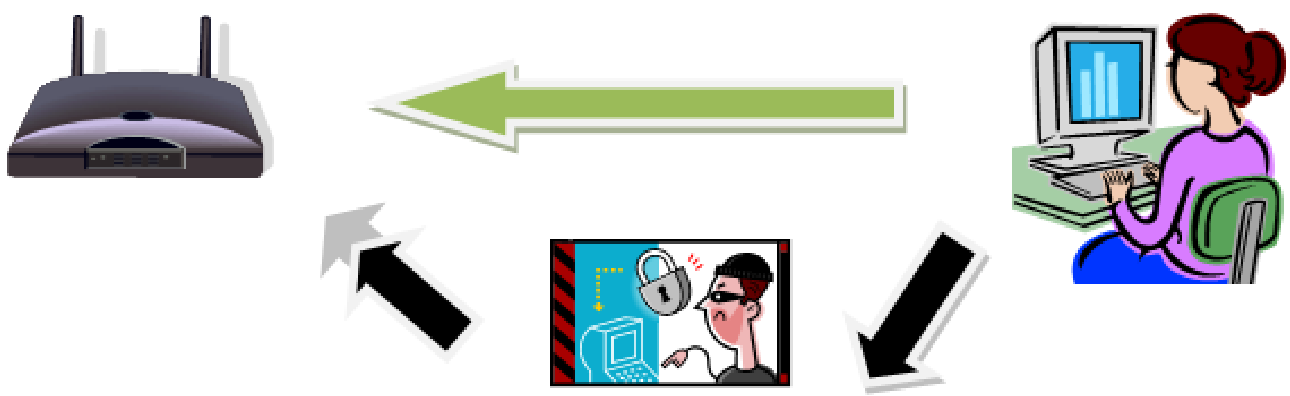



```
root@guvenlikod:/home/huzeyfe# echo "1" > /proc/sys/net/ipv4/ip_forward
root@guvenlikod:/home/huzeyfe#
```

Nemesis ile Arp Spoof Uygulaması

Ortam:

Gateway görevinde modem	192.168.1.1	00:13:64:22:39:3F
Masum Windows XP kullanıcısı	192.168.1.2	00-04-61-47-da-74
ARP Spoof yapacak Linux kullanıcısı	192.168.1.4	00:0c:29:08:e2:48



Nemesis Arp Spoofing-II

- Saldırı öncesi Windows sistemin arp tablosu.

C:\Console2>arp -a

Interface: 192.168.1.3 --- 0x4

Internet Address	Physical Address	Type
192.168.1.1	00-13-64-22-39-3f	dynamic
192.168.1.2	00-04-61-47-da-74	dynamic
192.168.1.4	00-0c-29-08-e2-48	dynamic

- Nemesis ile ARP Spoof

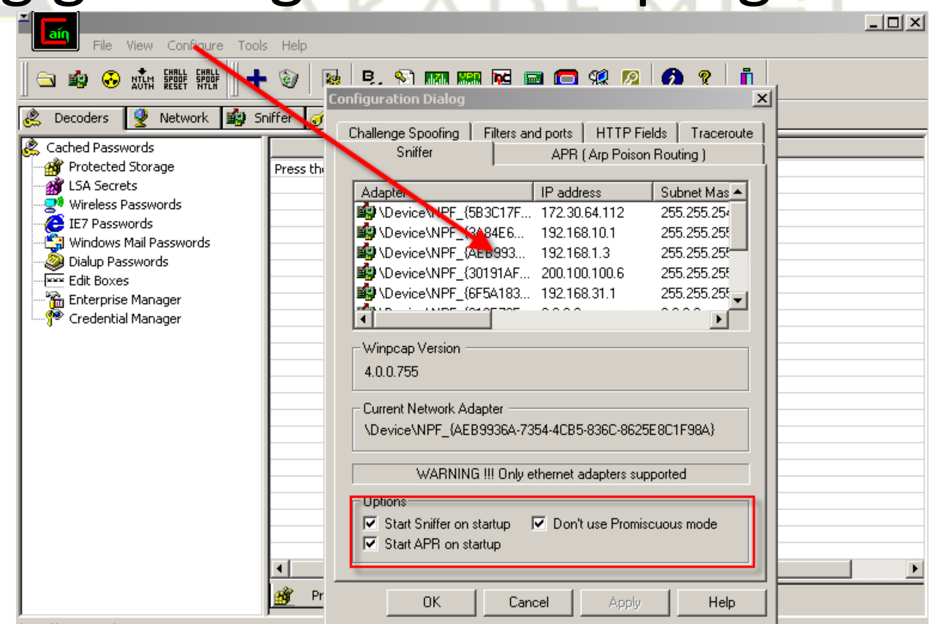
bt ~ # nemesis arp -d eth0 -r -v -S 192.168.1.1 -D 192.168.1.2 -h 00:0C:29:08:E2:48 -m 00:04:61:47:DA:74 -H 00:13:64:22:39:3f -M 00:04:61:47:DA:74

- *Windows makinenin ARP tablosuna tekrar bakılırsa 192.168.1.1 için ARP kaydının 00:13:64:22:39:3F'dan 00:0c:29:08:e2:48'a değiştiği görülecektir.*

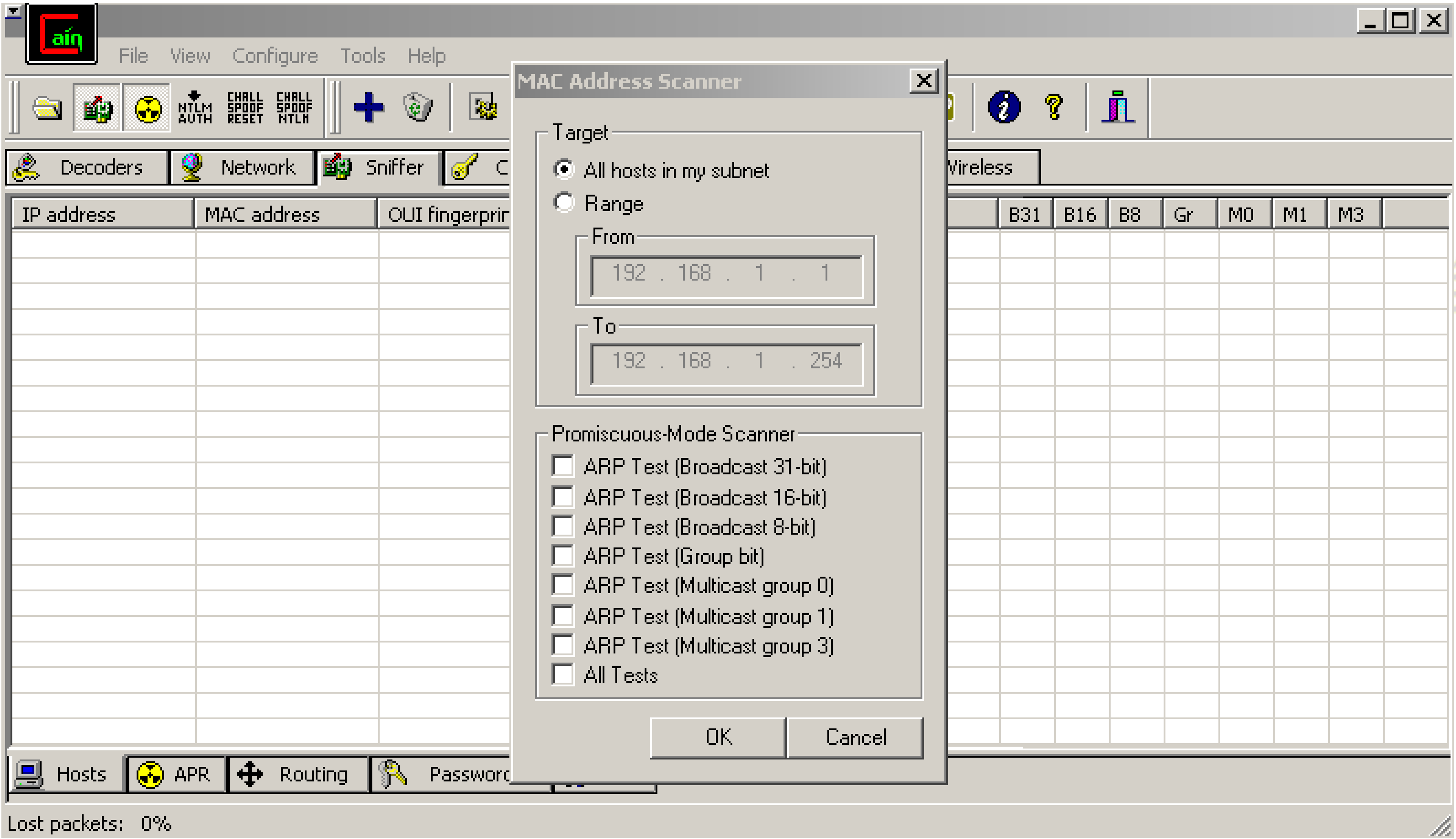
Cain&Abel ile ARP Poisoning

- Cain & Abel çok amaçlı bir Güvenlik aracıdır.
- Cain ve Abel olarak iki parçadan oluşur.
  - Bir parçası daha çok sistem ve parola işlemleri,
  - Diğeri parçası ise ağ güvenliği ile alakalı programlar içerir.

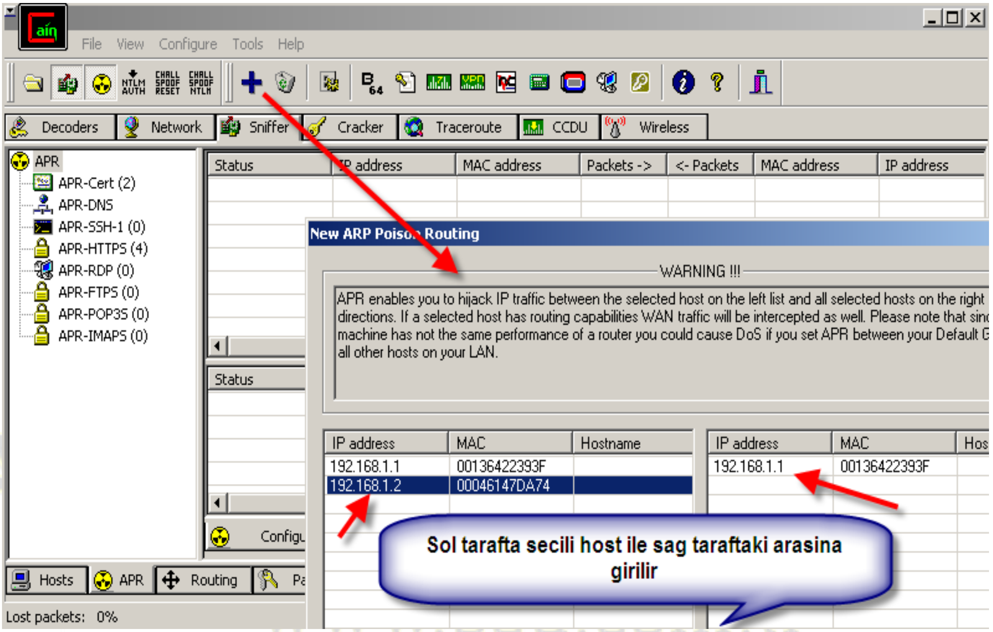
ARP spoof işlemi hangi arabirim üzerinden yapılacak?

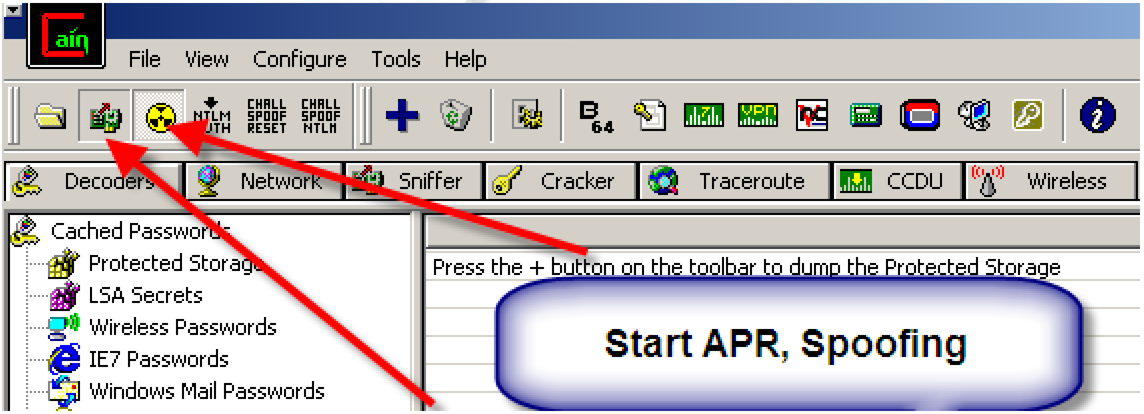


Cain&Abel ile Hedef Host Keşfi

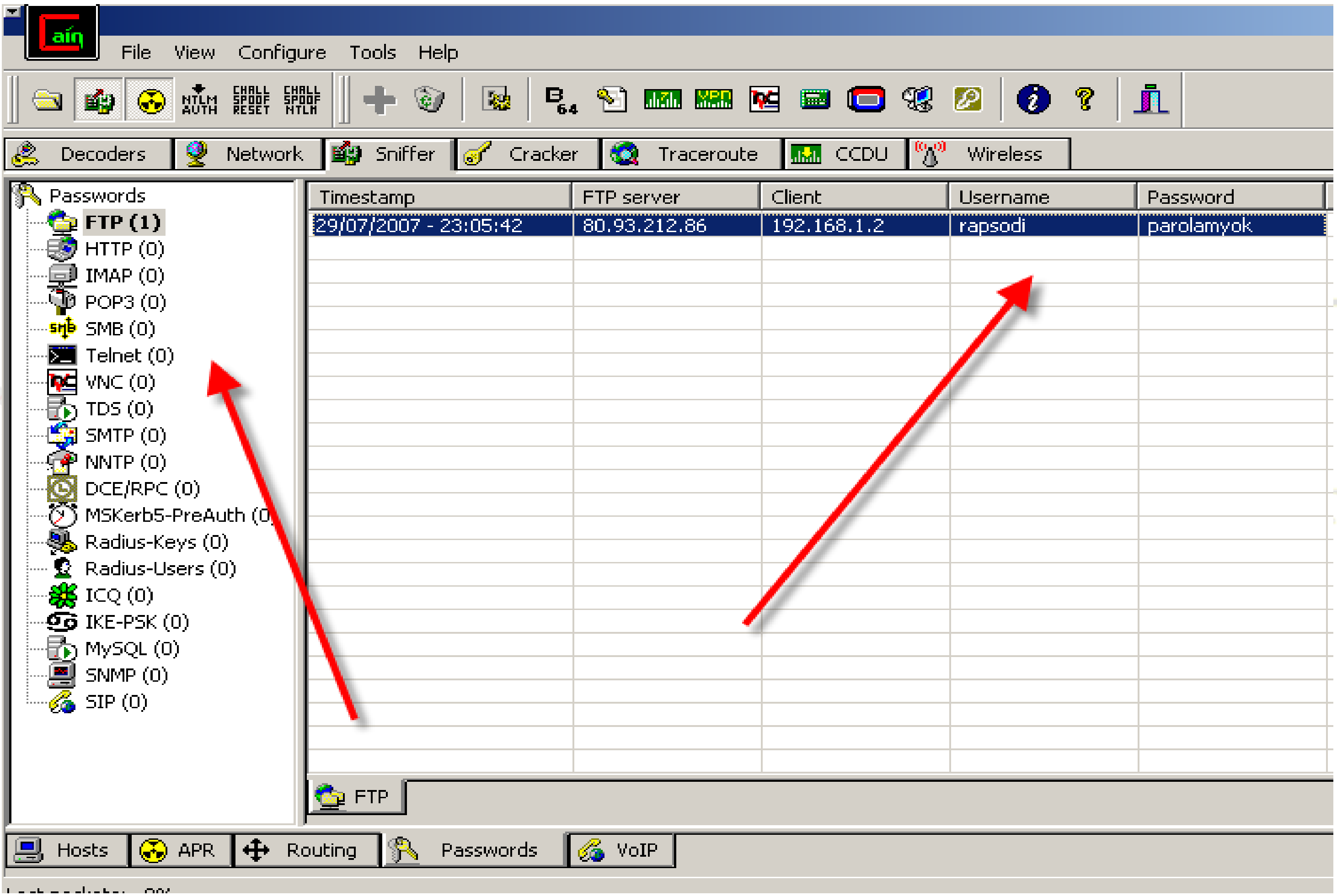


Hedef Seçimi





Kurbana Ait Parola Bilgilerini Görme



Ettercap : Gelişmiş Hijacking Aracı

- Ettercap, Linux ve Windows sistemlerde çalışan çok yönlü trafik dinleme, araya girme ve veri değiştirme aracıdır.
- TCP/IP'deki zayıflıklardan yararlanır.
- Komut satırı ve grafik arabirim seçenekleri

ettercap –C ile Curses modda çalıştırır

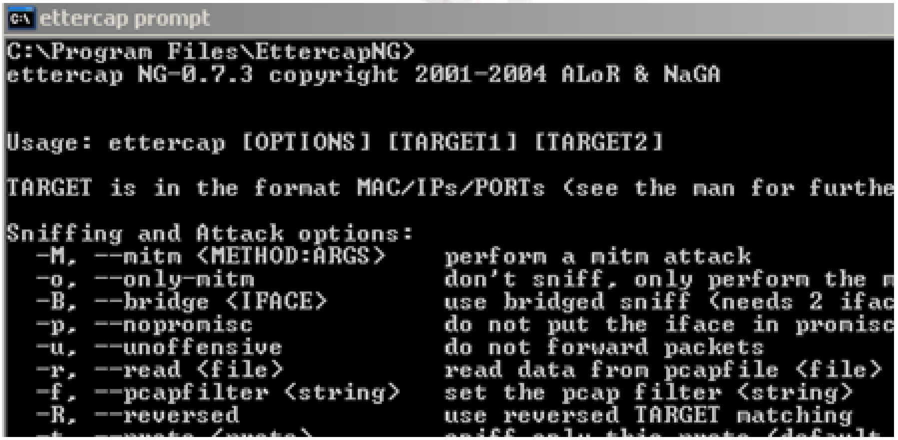
Ettercap –I interaktif modda çalıştırır.

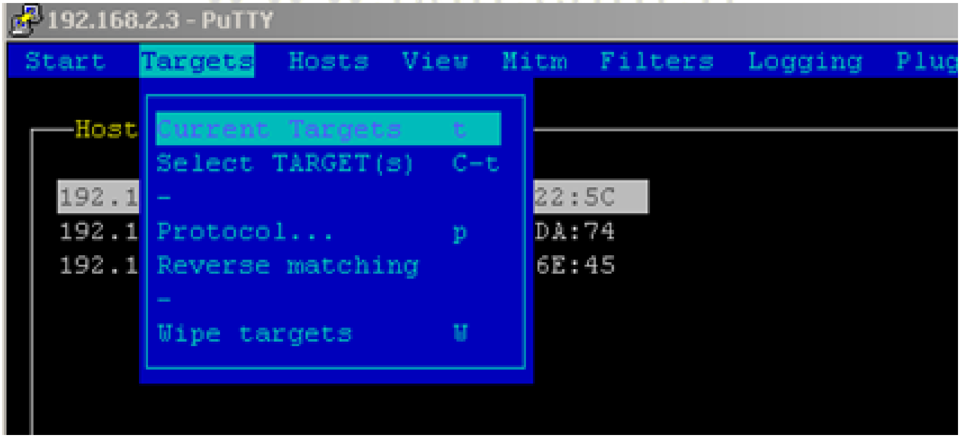
Temel Ettercap Özellikleri

- Kurulmuş bağlantılarda araya girme ve karekter sokuşturma,
- SSH1 bağlantılarında araya girme ve gizli bilgileri okuma,
- HTTPS bağlantılarında araya girme, değişiklik yapma,
- PPTP VPN bağlantılarında araya girme,
- Çeşitli protokoller için şifre toplama aracı
  - TELNET, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, HALF LIFE, QUAKE 3, MSN, YMSG.
- Araya girilen bağlantıları sonlandırma,
- Yerel ağlarda sniffer tespiti yapma,

Ettercap Çalışma Modları

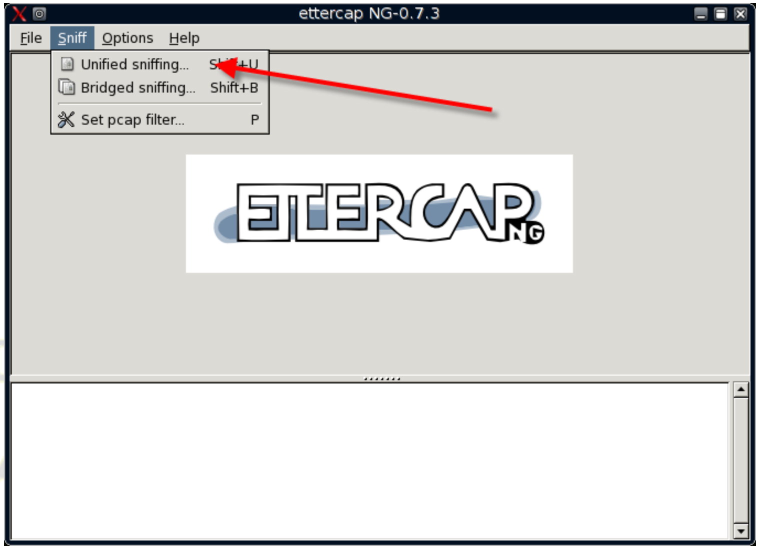
- Komut satırından kullanım
- Grafik arabirimli kullanım
- Ncurses text arabirimli kullanım

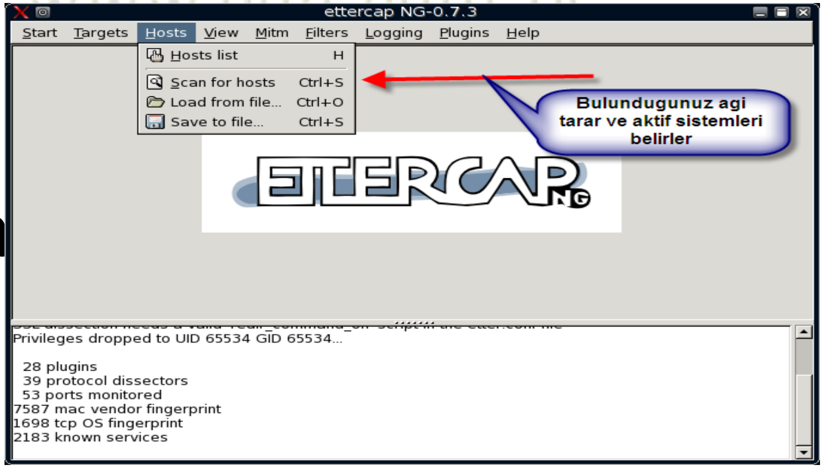




Ettercap Kullanımı

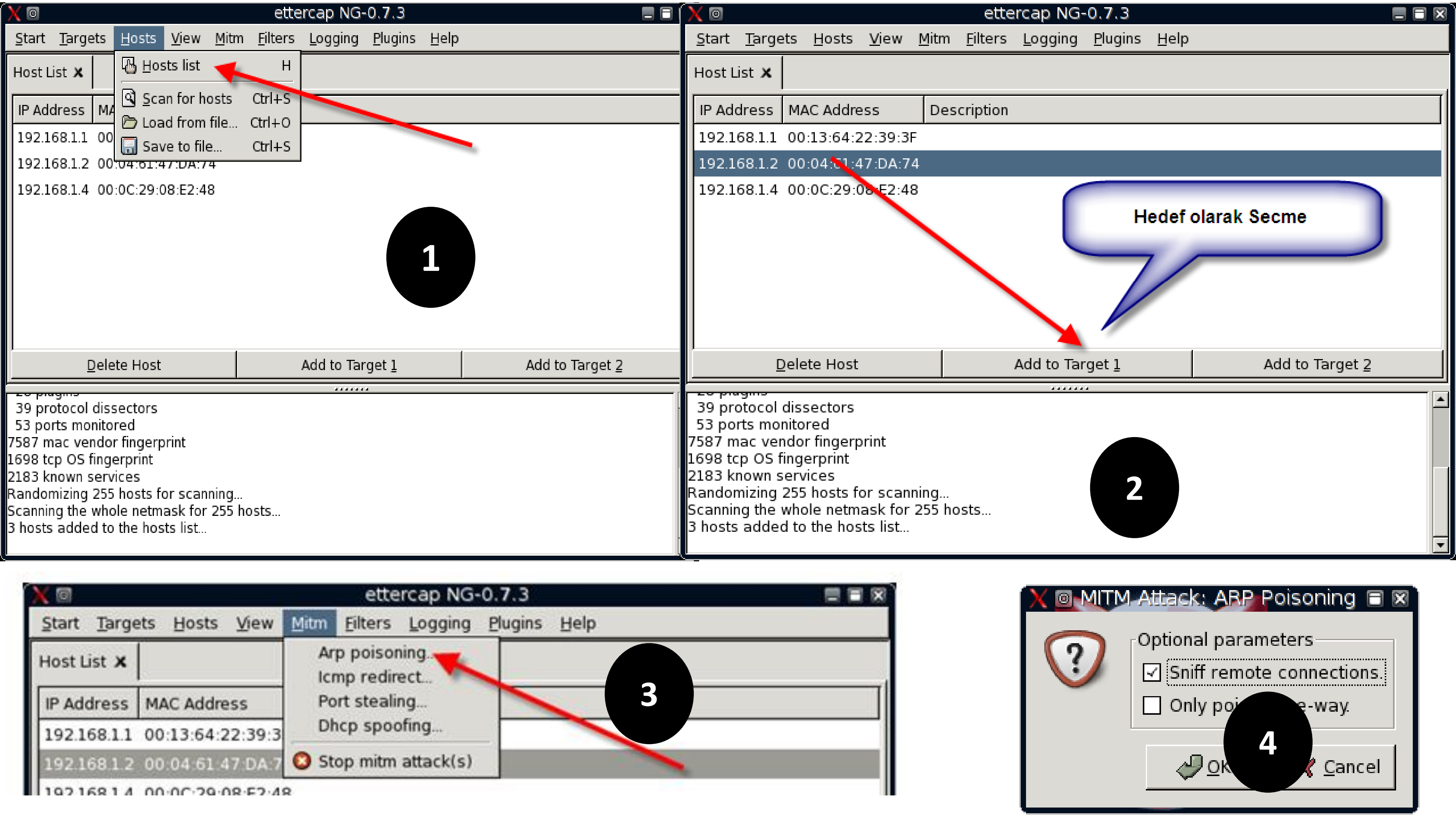
- İlk işlem hangi tür sniffing yapılacağının seçilmesi



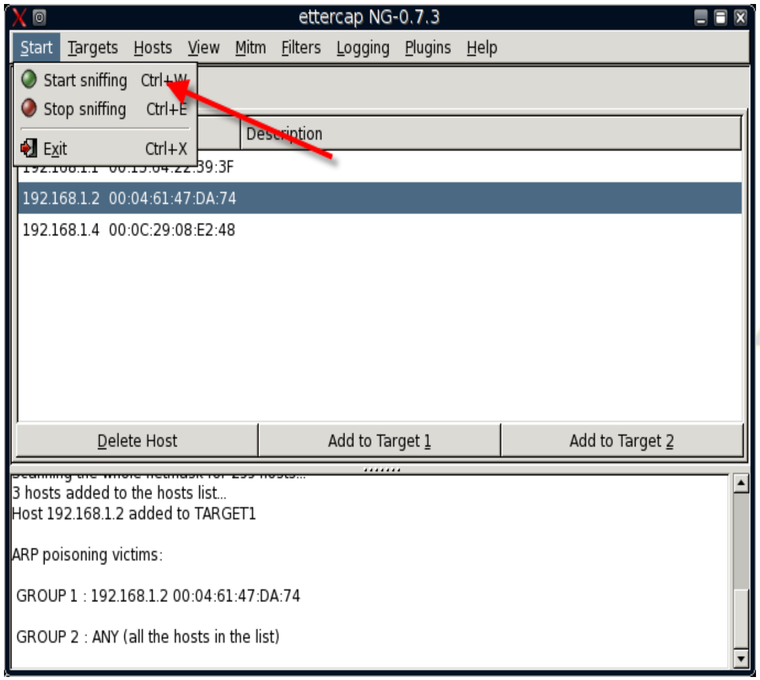


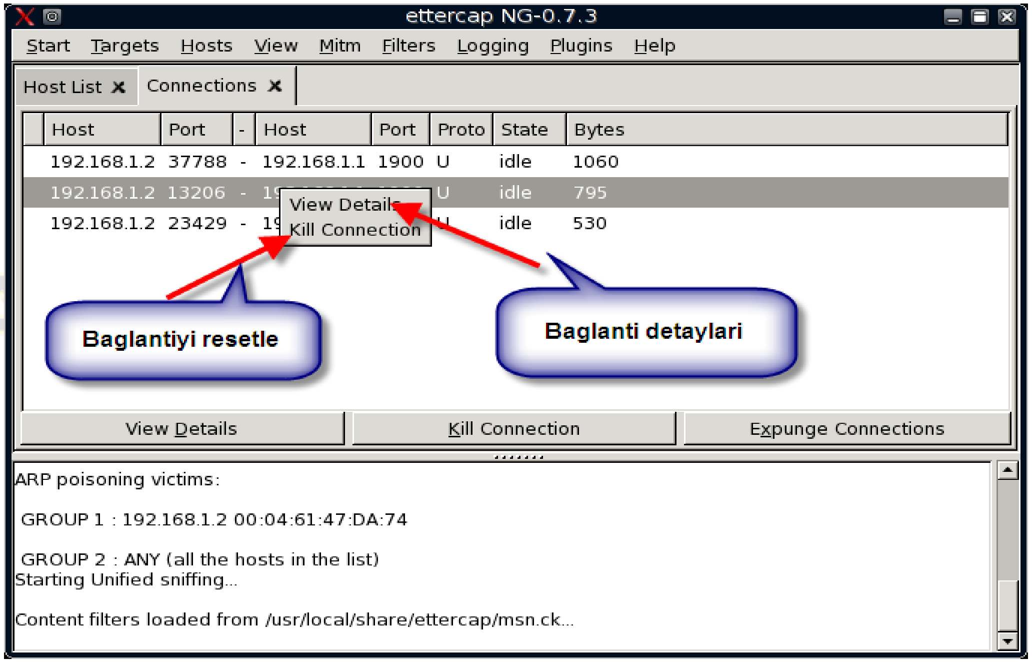
- Kurban sistem bulmak için Yerel ağ taraması yapılır.

Kurban Seçimi



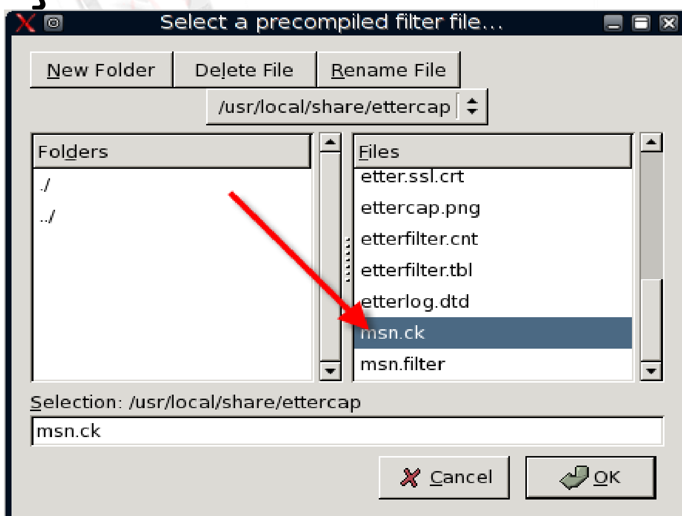
Bağlantıları Yönetme

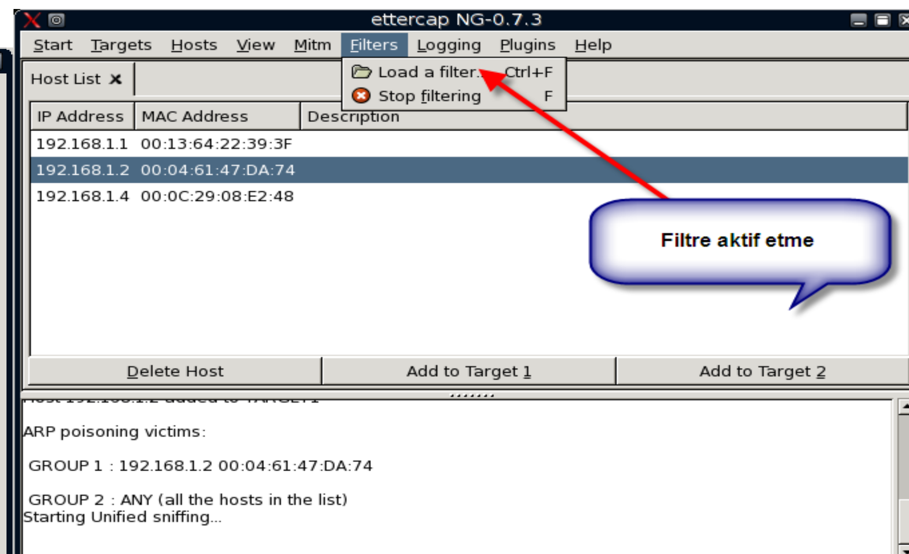




Ettercap Filtreleri

- Ettercap'in en güçlü olduğu yanlardan biri de akan trafikte filtreleme yapabilmesi ve bu filtrelemeye göre trafiği kaydedip değiştirebilmesidir.
- Mesela bir MSN görüşmesinde selam yazan mesajı araya giren kişi otomatik olarak salam'a dönüştürebilir.





TCP Paketlerinde Değişiklik Yapma

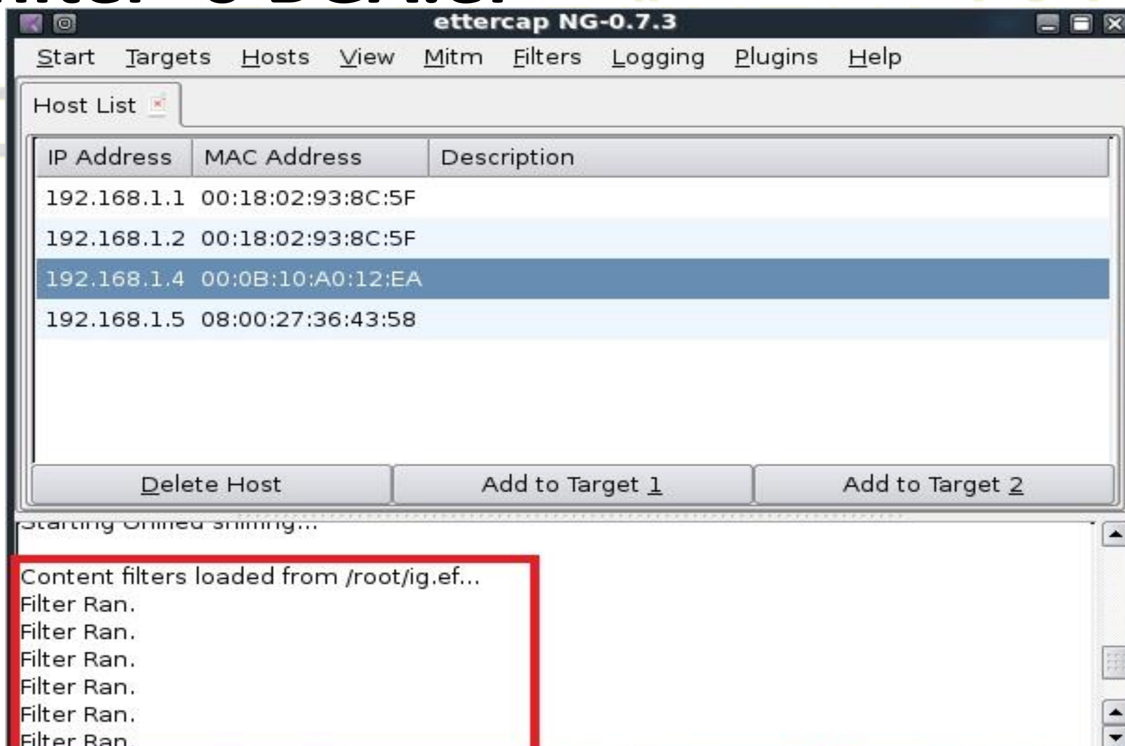
- Bga gördüğün paketleri BGA olarak değiştir.

```
if (ip.proto == TCP && search(DATA.data, “bga") ) {
  log(DATA.data, "/tmp/mispelled_ettercap.log");
  replace(“bga", “BGA");
  msg("Correctly substituted and logged.\n");
}
```

```
# log all telnet traffic, also execute ./program on every packet
if (ip.proto == TCP) {
  if (tcp.src == 23 || tcp.dst == 23) {
    log(DATA.data, "./logfile.log");
    exec("./program");
  }
}
```

Filtreyi Derleme

- Filtreyi oluşturmak için aşağıdaki komut kullanılabilir.
- **etterfilter bga.filter -o BGA.ef**



Ettercap: Uzak Sistemin Browserini Alma

- MITM ile araya girdikten sonra Ettercap kullanılarak hedef sistemin browserinı kendi sisteminizmiş gibi izleyebilirsiniz.
- Bunun için yapılması gereken değişiklikler
- /etc/etter.conf değişikliği

- *Bu değerler yerine*
  EC_uid =65534
  EC_gid = 65534
  bu değerleri ekle
  EC_uid = 0   #65534
  EC_gid = 0   #65534

- Mozilla yazan yeri firefox olarak değiştir./

Mozilla Firefox Değişimi

- Eski ayar:
  - remote_browser = "mozilla -remote openurl(http://%host%url)“
- Olması gereken ayar:
  - remote_browser = “firefox -remote openurl(http://%host%url)"

```
ettercap -T -Q -M arp:remote -i wlan0
/10.10.10.23/ // -P remote_browser
```

ARP Kullanarak DoS

- Yerel ağlarda kullanılen en temel protokol ARP’dır.
- ARP çalışma yapısı itibariyle korunmasız bir protokoldür.
- Alınan ARP-Reply paketlerinin doğruluğunu sorgulama mekanizması yoktur.
- Bir saldırgan sahte ARP cevap paketleri göndererek gatewayin MAC adresini istediği gibi gösterebilir ve yerel ağdaki iletişimi durdurabilir.
- Tek paket göndererek yerel ağın internet erişimi durdurulabilir.

ARP DOS-II

- Kurban Olarak bir Host/Network Seçilir
- Gateway IP Adresi Öğrenilir.
- Host'a/Network'e bozuk ARP-REPLY paketleri gönderilir.
  - Gateway 00:00:00:00:02:01 adresinde
- Host/Network ile Gateway arasında tüm iletişim durur!
- Uygulama

Nemesis ile ARP Dos Denemesi

- **#nemesis arp -d eth0 -r -v -S 10.2.0.1 -D 10.2.0.6 -H 00:01:02:03:04:05 -M 00:1B:38:C3:D3:A0**

Nemesi ARP DoS Çıktısı

ARP/RARP Packet Injection -=- The NEMESIS Project Version 1.4beta3 (Build 22)

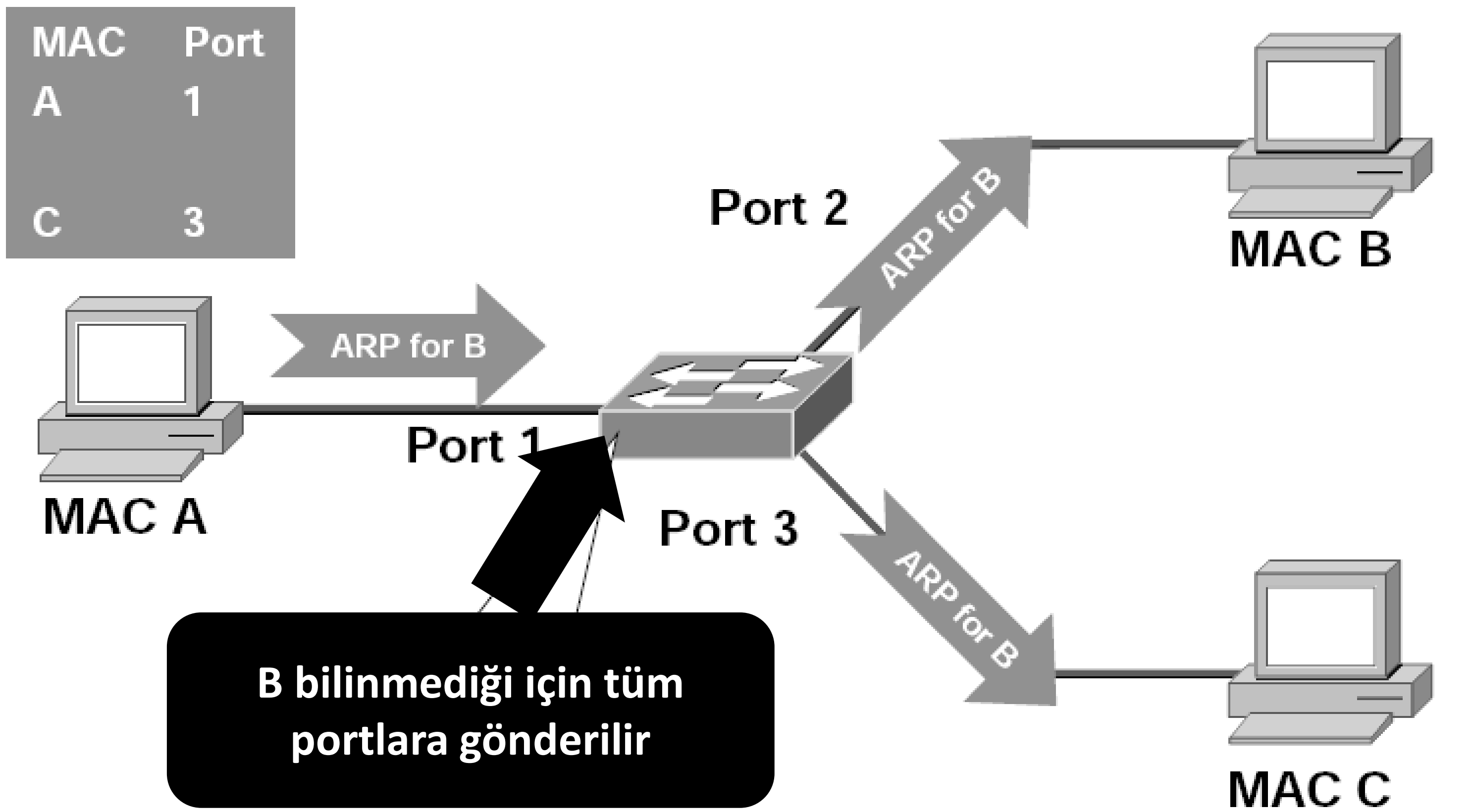
```
          [MAC] 00:01:02:03:04:05 > 00:1B:38:C3:D3:A0
   [Ethernet type] ARP (0x0806)

 [Protocol addr:IP] 10.2.0.1 > 10.2.0.6
 [Hardware addr:MAC] 00:01:02:03:04:05 > 00:1B:38:C3:D3:A0
     [ARP opcode] Reply
 [ARP hardware fmt] Ethernet (1)
 [ARP proto format] IP (0x0800)
 [ARP protocol len] 6
 [ARP hardware len] 4
```

Wrote 42 byte unicast ARP request packet through linktype DLT_EN10MB.

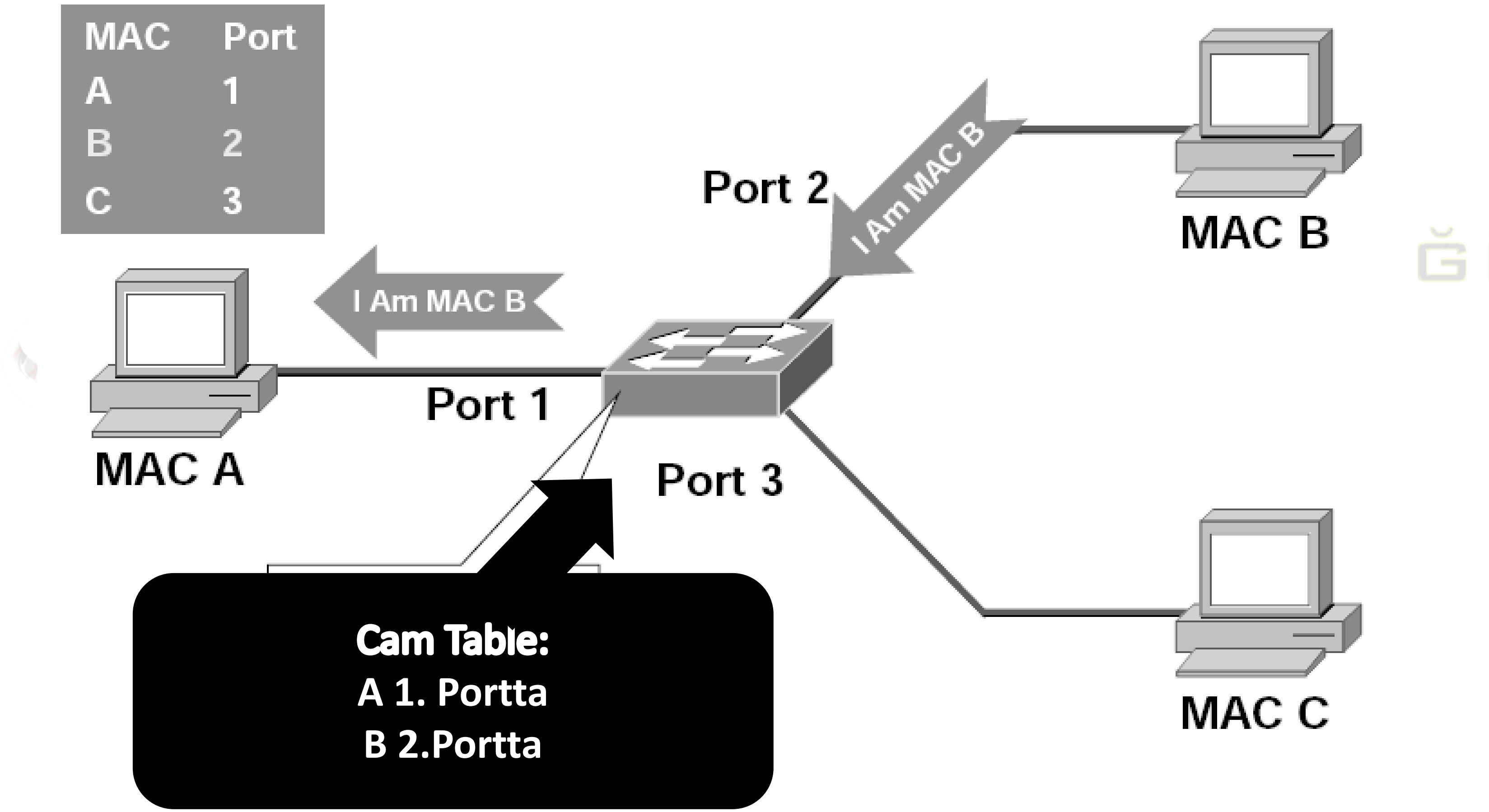
MAC Flooding

- Amac switch mantığını bozup sistemin bir hub gibi çalışmaya zorlamak.
- Switch Cam Table(Port-Mac Bilgilerini Tutar)
- Etherflood ve Macoff yazılımları kullanılabilir.

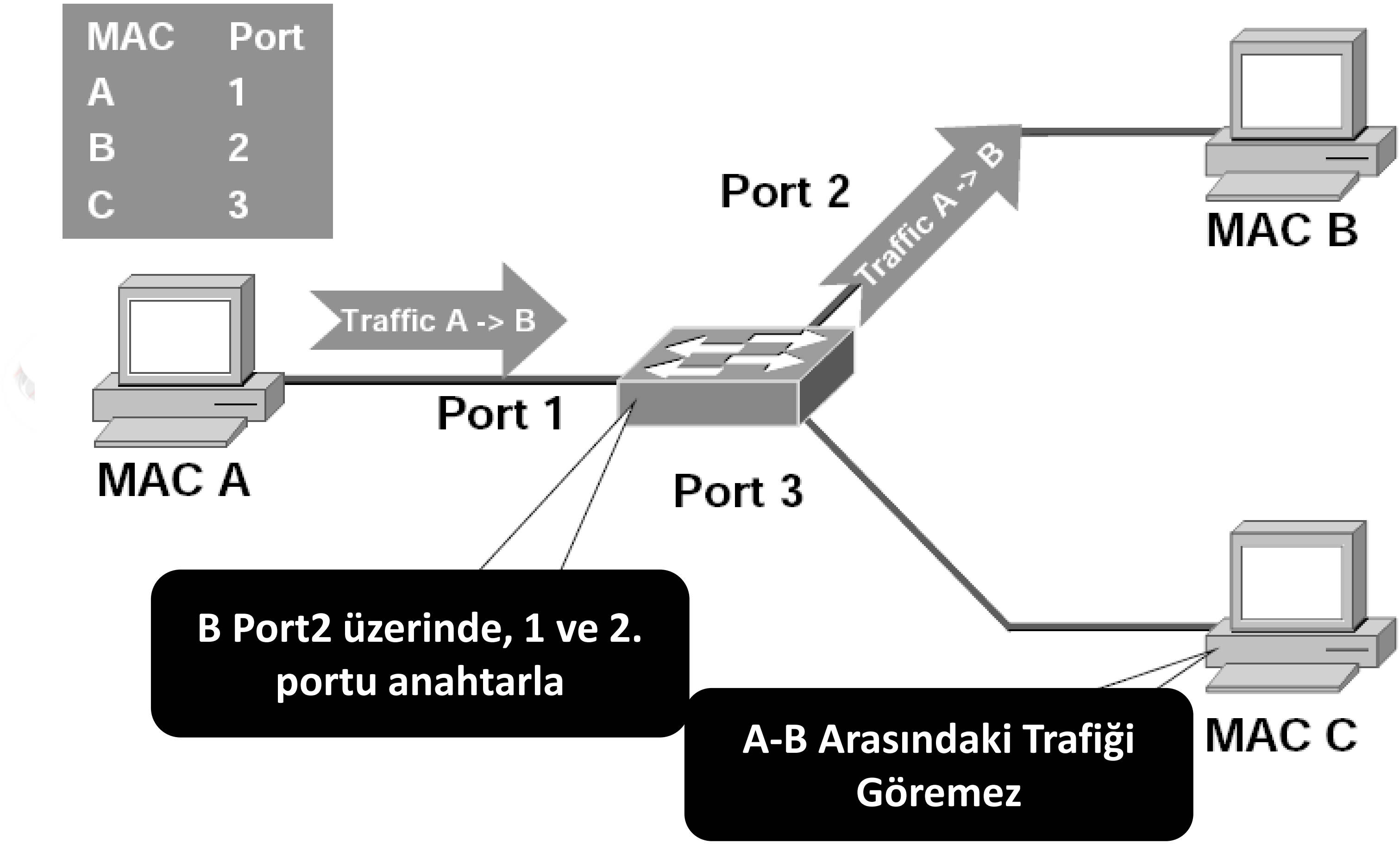
Cam Tablosu-1



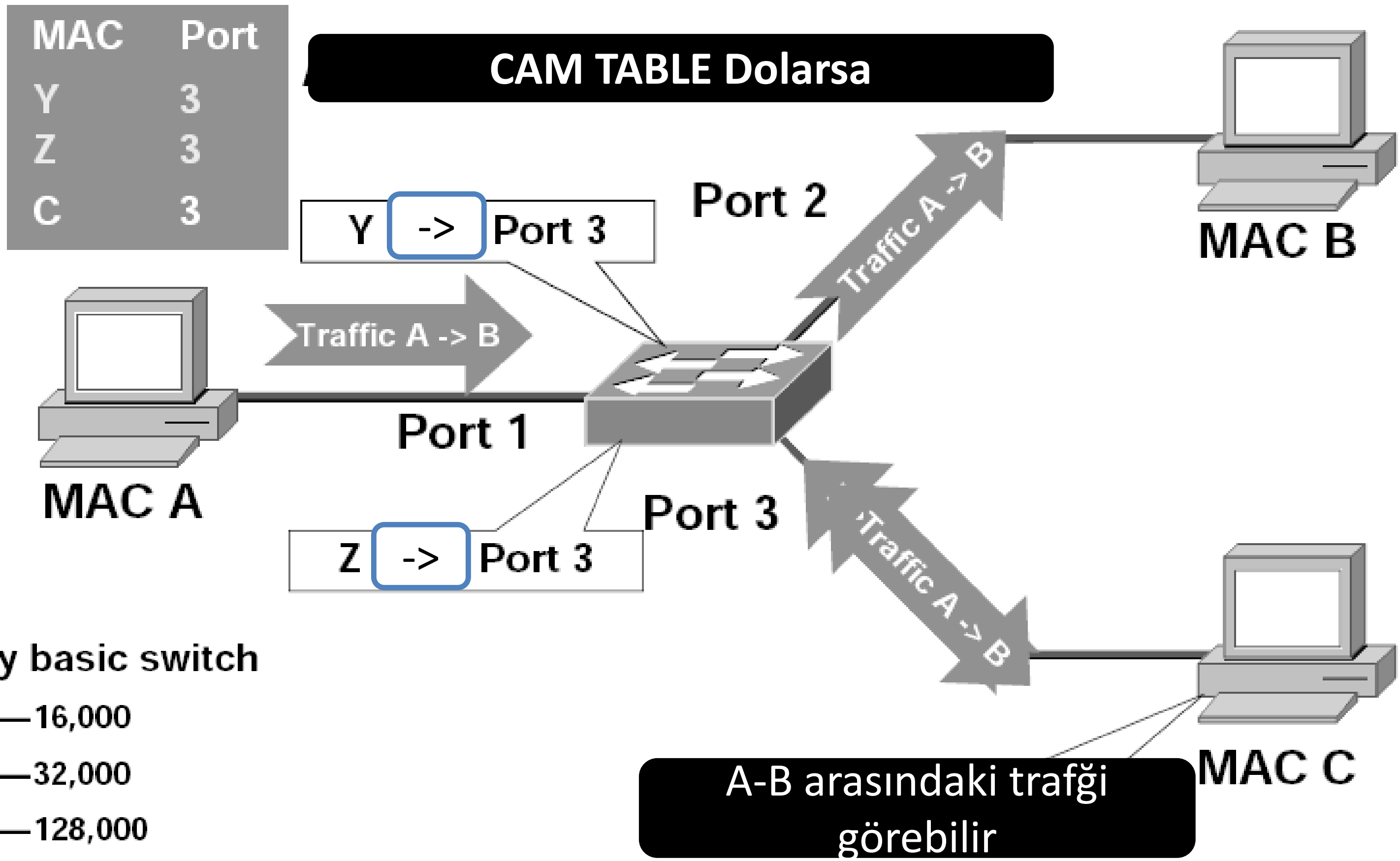
Cam Tablosu-2



Cam Tablosu-3



Mac Flood >Cam Overflow



Size by basic switch

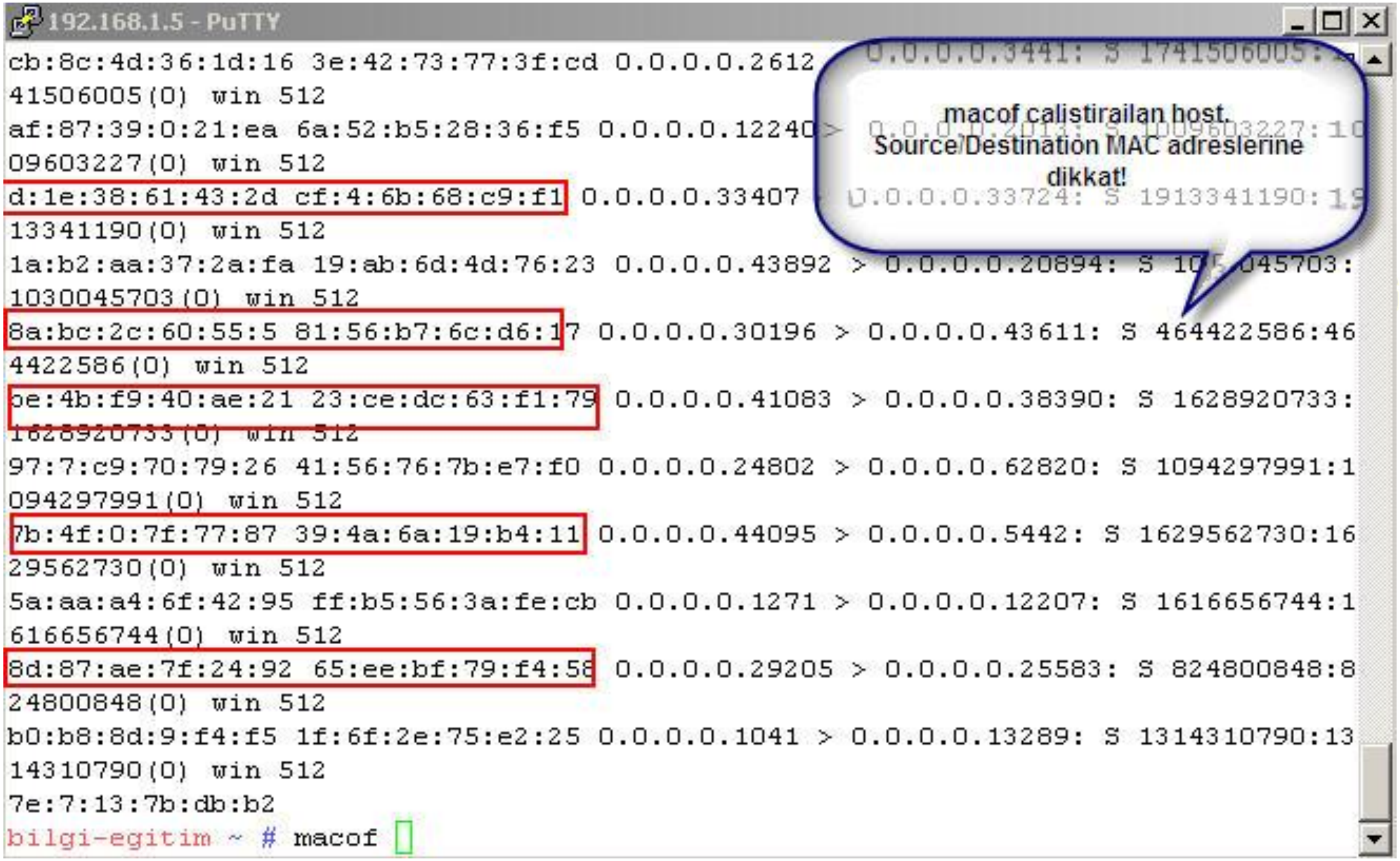
3xxx—16,000

4xxx—32,000

6xxx—128,000

"macof -i eth1 2> /dev/null"

Macoff ile Mac Flooding



ARP Saldırılarından Korunma

- Temelde iki tür koruma vardır:
  - Statik koruma yöntemleri.
  - Dinamik koruma yöntemleri.
- Arpwatch
- Arpalert yazılımları
- “Ip-Mac ikililerini bir dosyaya yaz, herhangi bir değişiklik olursa uyarı ver” mantığıyla çalışır.
- Statik ARP kaydı girilmesi

ARP Saldırılarına Karşı Korunma

- Statik ARP kayıtları
  - İşletim sistemine erişmek istediği kaynaklar için(genellikle gateway) sabit MAC adresi tanımı yapılması,
  - Sabit MAC adresi tanımı sonrası sisteme gelecek arp-reply paketleri sistemdeki ARP cache’I ile oynama yapamaz.
  - Tek yönlü olduğu için gerçek bir koruma sağlamaz.
- Kullanılan Switch üzerinde koruma yöntemlerinin aktif edilmesi
  - DHCP Snooping
  - Source Guard
  - Dynamic ARP Inspection

Statik ARP Kaydı Girme

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Giga-Byt_5a:1b:96	Cisco-Li_f1:33:2e	ARP	Who has 192.168.1.1? Tell 192.168.1.100
2	0.000301	Cisco-Li_f1:33:2e	Giga-Byt_5a:1b:96	ARP	192.168.1.1 is at 00:22:6b:f1:33:2e
3	2.140460	192.168.1.100	192.168.1.111	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=1/256, ttl=128)
4	6.176059	Cisco-Li_f1:33:2e	Giga-Byt_5a:1b:96	ARP	Who has 192.168.1.100? Tell 192.168.1.1
5	6.176092	Giga-Byt_5a:1b:96	Cisco-Li_f1:33:2e	ARP	192.168.1.100 is at 00:1f:d0:5a:1b:96
6	6.999884	192.168.1.100	192.168.1.111	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=2/512, ttl=128)

Arp –s ip_adresi mac_adresi

```
captured (592 bits)
Ethernet II, Src: Giga-Byt_5a:1b:96 (00:1f:d0:5a:1b:96), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
  Destination: Cimsys_33:44:55 (00:11:22:33:44:55)
    Address: Cimsys_33:44:55 (00:11:22:33:44:55)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  Source: Giga-Byt_5a:1b:96 (00:1f:d0:5a:1b:96)
  Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.111 (192.168.1.111)
Internet Control Message Protocol
```

Administrator: C:\Windows\System32\cmd.exe

```
C:\Windows\system32>arp -s 192.168.1.111 00-11-22-33-44-55

C:\Windows\system32>ping 192.168.1.111 -n 2

Pinging 192.168.1.111 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.1.111:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

C:\Windows\system32>
```

Statik ARP Kaydl girme

Statik ARP Kaydı Önlemini Atlatma

- Statik ARP Kaydı sadece istemci ile Router arasındaki trafiği tek yönlü olarak korumaya alır.
  - İstemciden Router'a gidecek paketleri saldırgan ARP kayıtlarını değiştiremediği için okuyamaz
- Saldırgan Router'dan istemciye dönecek olan paketleri Router'i kandırarak kendi üzerinden geçirebilir.
  - Router üzerine statik ARP kaydı girilmediği müddetçe saldırgan tek yönlü olarak trafiği inceleme hakkına sahiptir.
- Tek yönlü trafikte user/pass bilgileri olmasa da sunucudan dönen cookie/session gibi bilgiler yer alabilir.

DHCP Snooping

- DHCP istemi ve sunucu arasında görünmez güvenlik duvarı işlevi
- Sahte DHCP sunucu engellemek için
- DHCP'den gelen dogrulamış cevapları bir tabloya kayıt eder ve ARP spoof engellemeleri için kullanılabilir.
- Her VLAN için ayarlanabilir
- Her switch için farklı yapılandırma parametrelerine sahiptir.

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/snoodhcp.html

IDS/IPS Sistemler ve ARP Spoofing

- IP-MAC eşleşmesi gerçekleştirerek bir tablo oluşturulur.
- Bu tablodaki düzeni bozacak her paket için uyarı verilir.
- Örnek Snort IDS Yapıladırımı

```
#  SID     Event description
# -----   -------------------
#   1      Unicast ARP request
#   2      Etherframe ARP mismatch (src)
#   3      Etherframe ARP mismatch (dst)
#   4      ARP cache overwrite attack

#preprocessor arpspoof
#preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00
```

Arpwatch

- Arpwatch açık kaynak kodlu ARP faaliyet izleme programıdır.
- Yerel ağda çalıştırıldığında tüm ARP paketlerini izleyerek MITM ya da benzeri türde anormallikleri tespit edebilir.

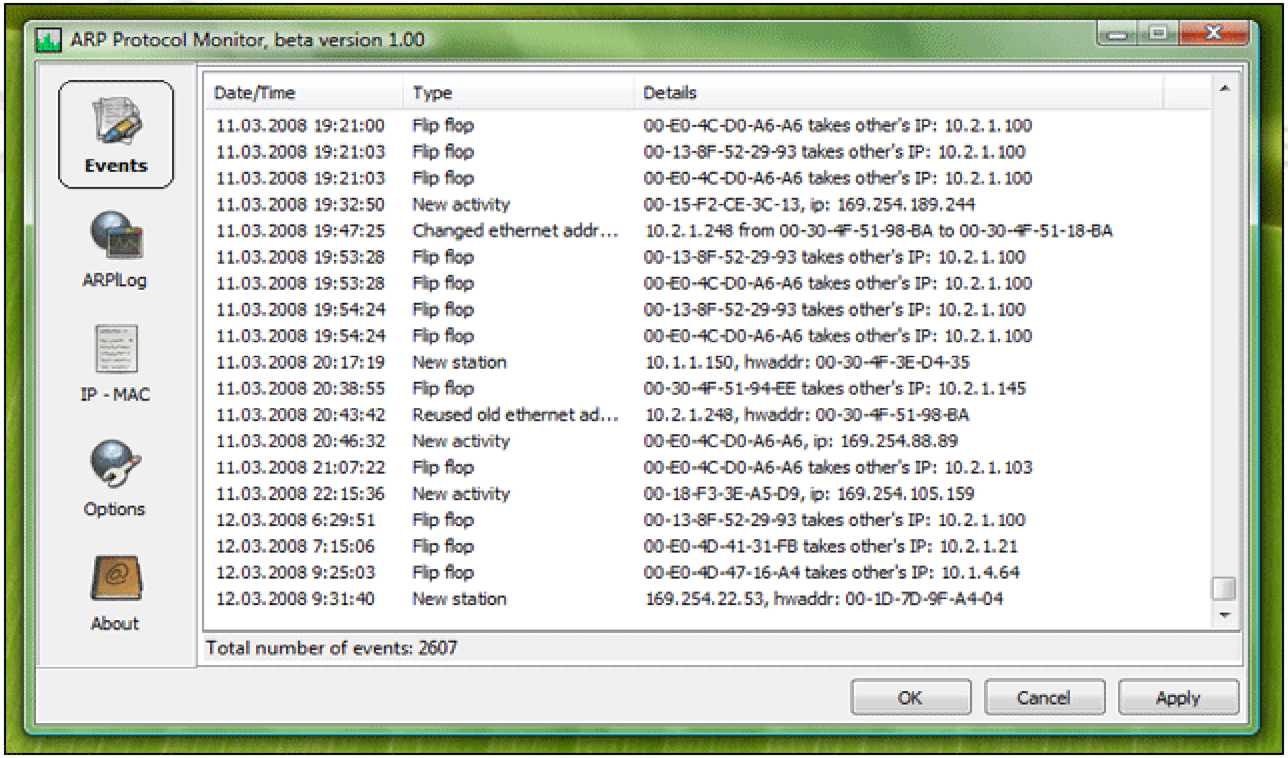
```
#  cat messages | grep ’192.168.2.33’
Aug 14 18:05:49 ver arpwatch: bogon 192.168.2.33 0:2:6f:46:74:f
Aug 14 18:05:54 ver arpwatch: bogon 192.168.2.33 0:2:6f:46:74:f
Aug 14 18:06:05 ver arpwatch: bogon 192.168.2.33 0:2:6f:46:74:f
Aug 14 18:06:31 ver arpwatch: bogon 192.168.2.33 0:2:6f:46:74:f
```

Arpwatch Kurulumu

```
root@bt:~# apt-get install arpwatch
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  arpwatch
0 upgraded, 1 newly installed, 0 to remove and 39 not upgraded.
Need to get 185kB of archives.
After this operation, 647kB of additional disk space will be used.
Get:1 http://32.repository.backtrack-linux.org/ revolution/main arpwatch 2.1a15-1.1
[185kB]
Fetched 185kB in 0s (320kB/s)
Selecting previously deselected package arpwatch.
(Reading database ... 226895 files and directories currently installed.)
Unpacking arpwatch (from .../arpwatch_2.1a15-1.1_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for ureadahead ...
Setting up arpwatch (2.1a15-1.1) ...
Starting Ethernet/FDDI station monitor daemon: (chown arpwatch
/var/lib/arpwatch/arp.dat) arpwatch.
```

BinaryPlant ARP Monitor

- ARP değişikliklerini Windows ortamında loglayan ve alarm üreten çeşitli yazılımlar bulunmaktadır.



BGA İletişim

www.bga.com.tr

blog.bga.com.tr

twitter.com/bgasecurity

facebook.com/BGAkademisi

bilgi@bga.com.tr

egitim@bga.com.tr