Trafik Analizinin Belirlenmesi ve Engellenmesi

/***
Bâkır EMRE *
* emre [at] enderunix [dot] org *
* EnderUNIX Yazılım Geliştirme Takımı *
* http://www.enderunix.org *
*
* Sürüm : 1.0 *
* Tarih : 04.06.07 *
* Etiketler : sniff,promiscuous,unix,security,ids *
* Seviye : Orta Seviye *
* Makalenin en yeni versiyonu : http://www.enderunix.org/docs/trafikAnaliziBelirlemeEngelleme.pdf *
* adresinden elde edilebilir. *
***/

İçindekiler

Özet

Günümüzde gerek kablosuz ağların artmasıyla gerekse sisteme zarar vermek isteyen yada meraklı kullanıcıların ortamda neler olup bittiğini görmek için ağ trafiğini dinlemek istemektedirler. Bu durumda ağdaki paket dinleyicilere karşı önlem almak gerekmektedir.
Bu makalede ağ trafiği analizi yapan snifferlar (paket dinleyicileri) ve bunlardan nasıl veriler elde edilir, tesbiti nasıl yapılır ve korunmak için neler yapılması gerektiği anlatılmaktadır.

Anahtar kelimeler :

Paket dinleme, arp spoof, güvenli kanallar

1.Giriş

Ağ teknolojilerinin gelişmesi ile birlikte ağ güvenliği daha önemli hale gelmiştir. Ağ trafiği analizi yapılarak ağ trafiği analizinin ehil olmayan yada sisteme sızmak veya zarar vermek isteyen kişilerce yapılaraktan ulaşmak istedikleri verileri elde etmeleri güvenlik kavramını iyiden iyiye artmasi anlamina gelmektedir.

2.Paket Dinleyiciler

Paket dinleyici ağ trafiğini gizlice dinleyen ağ üzerinde dolaşmakta olan verileri yakalamak için kullanılan yazılıma verilen isimdir. [6]. Yada bilgisayar ağına konarak ağ trafiğini gizlice dinleyen araçlara denir. Tanımlardan da anlaşıldığı gibi paket dinleyicileri yazılım yada donanım olabilmektedir. Bu bağlamda paket dinleyicileri için "veri yakalama teknolojisi" olarak bahsedilmesi pek doğru olacaktır.

Trafik analizinin yapılmasını aşağıdaki şekilde guruplayabiliriz.

- Bilinmeyen Protokol Analizi:

  Burada kullandıgığımız bir uygulamanın kullandığı protokol nasıl işliyor nasıl çalışıyor? bilgisini elde edebiliriz.

  Örneğin SIP protokolü üzerinde çalışan VoIP uygulamasinin çalışırken session hangi portlardan kurulur. Veri aktarımı hangi port üzerinden devam eder. Böyle bir yapıyı çözebilmek için protkol analizi yapabiliriz.

- Ağ trafiği başarımı

  Kullandığımız cihazların ağ trafiği için ne kadarverim alınaabiliyor ne kadarını
  Örneğin 100Mbit bir hattın ne kadar bir verim elde ediyoruz.

- Anormal trafik gözleme

Ağa yapılacak herhangi bir saldırıyı tebşt etmek için
Örnek: port tarama vs

- Firewall/IDS/IPS altyapısı.

  Firewall ve IDS/IPS sistemlerinin altında ağ trafiği analizi yatar

- Sistem açıklıklarının bulunması

Paket dinleyici niye kullanılır sorusunu açıklamak için Paket dinleyicileri kimler kullanır sorusuyla birleştirerek açıklamaya çalışırsak

- Iyi / Ağ yöneticileri= Protokol analizi
- Kötü / Hacker?=Açıklık varmı?
- Geliştiriciler = Uygulamam doğru çalışıyormu?
- Kullanıcılar/Meraklılar

Ağ yöneticileri.

- Ağ içerisindeki darboğazları bulmak için
- Ağ performansını ölçmek için
- Ağ daki hataları bulmak için
- Ağa yapılan nüfûz ve atakları gözlemlemek için
- Ağı korumak ve ayakta tutmak için

Hackerlar

- Ağda, şifrelenmeden giden-gelen kullanıcı adı-şifreler kredi kartı bilgileri vs.. aramak
- Açık port - servis aramak
- Ağ trafiğini okunabilir bir formatta elde ederek verileri kolayca eldeetme

Yazılım Geliştiricileri

- Yapmış oldukları ağ uygulaması düzgün çalışıyormu, paketler ulaşması gereken hedefe ulaşabiliyormu
- Paket içerikleri doğru olarak oluşturulmuşmu.

2.1 Paket dinleyicilerin zararları

Internetin ilk yıllarında geliştirilen Protokoller güvenlik tarafı düşünülmeden yapılmıstı. Bu protokoller üzerinde iletişim plain text olarak gitmektedir. [4]
Bu protokolere örnekler:

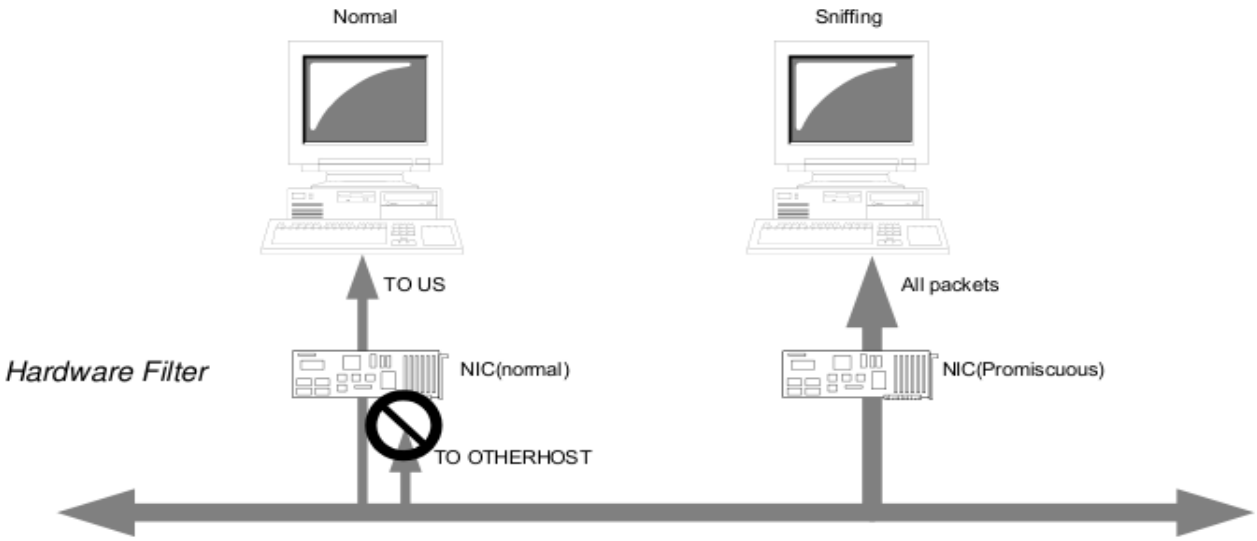
- Telnet

- FTP
- SMTP
- POP
- HTTP
- IMAPv4
- Rlogin

Başka bir tehlike trafik analizi yaparak önemli maillerin içeriğinin yanlış kişiler tarafından elde edilmesi. Yada Anında mesajlaşma programlarının içeriğinin gözlenmesi. Bir şirket için yukarıdaki bilgilerin elde edilmesi sonucu en çok rakiplerin işine yarayacaktır.

Öncelike bir kavramın bilinmesinde çok önemli burada: **Promiscuous mod**

2.2 Pomiscuous mod



Şekil 1 Promiscuous mod

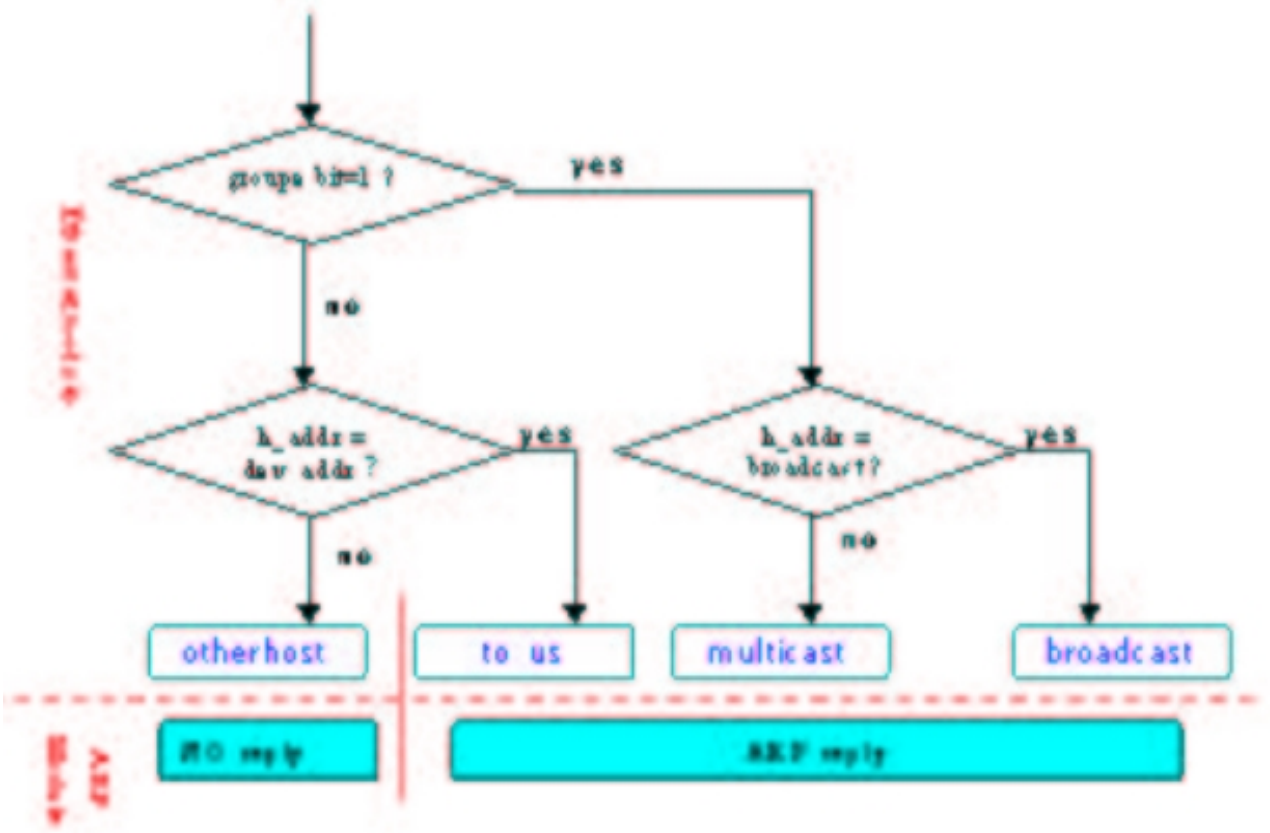
Hub kullanan ağlarda ağ arayüzü bütün ethernet framelerini kabul etmesine "Promiscuous mode" denir [Şekil 1] Burada bilgisayar ağdaki herşeyi dinlemesine izin verir yani kendisiyle alakalı olmayan paketleride dinlemek isteyecektir. Yani hedef adresini kontrol etmeden ağdaki bütün paketleri kabul eder[8]

Ethernet kartı üzerinde bir filtreleme mekanizması çalışmaktadır buna göre paketler varış MAC adresine göre sınıflara ayrılmaktadır
Bunlar

- Unicast paketler
  Tekbir yöne giden paketler bunlarıda şu şekilde gruplara ayırırsak
  - bize gelen paketler (to_us)
  - başkalarına giden paketler (to_others)

- broadcast paketleri
  Ağdaki bütün hostlara giden paketler
- multicast paketleri
  Multicast grubuna dahil olan hostlara giden paketler

Aşağıdaki diyagramda ethernet kartı üzerindeki filtreleme mekanizmasının gönderilen ARP paketine göre nasıl tepki verdiğini göstermektedir. [Şekil 2]



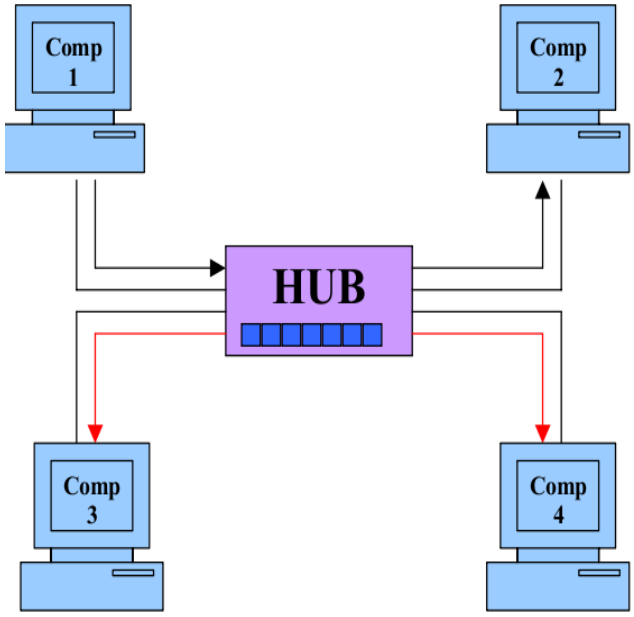
Şekil 2. Donanım Filtresi

Burda görüldüğü gibi ağ arayüz kartı varış adresine göre paketleri gruplamaktadır. Grup bitleri 1 olan paketler ya multicast yada broadcast paketleridir bu paketlerin geçmesine izin ver. Eğer grup bitleri 1 değilse o zaman bu paketin varış adresi bizim donanım adresimiz ise bu paketin geçmesine de izin ver. Diğer türlü bu paket başkalarına giden unicast paketleri olacaktır dolayısıyla bu paketin arp cevabını döndürme gibi bir mekanizma işleyecektir.

Burada gösterilen promiscuous yapı shared Ethernet topolojisi üzerinde gösterilmiştir yeri gelmişken bu yapılarıda açıklamak gerekir

2.3 Shared Ethernet

Shared Ethernet ortamında bütün hostlar birbirlerine aynı veri yolu üzerinden bağlıdır. [Şekil 3]Ve herbiri diğerinin bantgenişliği için yarışır Böyle ortamlarda paketler diğer makinalara ulaşır. Fakat herbir host üzerindeki donanım filtesi yukarıda açıkladığımız paketlerden türlerindeki geçirmektedir (bize gelen paketler (to_us), broadcast paketleri, eğer multicast grubuna dahilse multicast paketleri) [5]

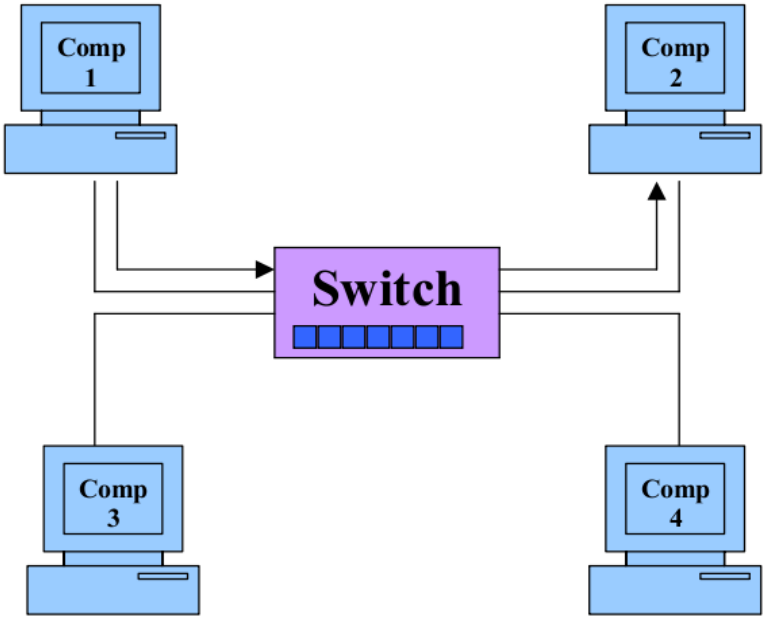


Şekil 3 Shared Ethernet

2.4 Switched Ethernet

Hub yerine Switchle birbirine bağlı olan ortamlara verilen isimdir. Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımlarından biridir.[Şekil 4] OSI yedi katman modelinin 2. katmanında, yani veri bağ katmanında, MAC adreslerini taban alarak portlar arasında veri iletme işlemi yapar. Ağ anahtarının her bir kapısı diğerlerinden bağımsız veri alış-verişinde bulunabilir. Bir veri paketi (veri çerçevesi) kapılardan birine ulaştığında ağ anahtarı gönderenin MAC adresini ve gönderilen kapıyı adres tablosuna kaydeder. MAC adres tablosundaki mevcut kayıtlar incelenerek hedef MAC adresinin bağlı olduğu kapıyı tespit etmeye çalışır. Eğer herhangi bir kayıt bulunamazsa, veri paketi gelen kapı hariç bütün kapılara gönderilir. Eğer MAC adresi biliniyorsa, bu durumda veri paketi sadece hedef kapıya gönderilir. Eğer gönderenin ve alıcının MAC adresleri aynıysa paket silinir. [5]

Switchler sadece hedef makinaya paketleri gönderir hublardaki gibi broadcast yaparak bütün bilgisayarlara göndermez Böylece ağ performansıda artmaktadır. Promiscuous mod burada çalışmamaktadır. Bundan Dolayı birçok sistem yöneticisi Switchli ortamlarda snifferların çalışmayacağını varsaymaktadırlar Peki bu doğrumudur?



Şekil 4 Switched Ethernet

Switchler MAC-adreslerini hafızada bir tabloda tuttarlar ve bu hafıza sınırlıdır. Bu tabloyu garbage MAC adresleriyle doldurarak switchin tablosını doldurup görevini yapması engellenebilir böylece switch hub gibi çalışmasına zorlanabilir Bu yöntem **MAC Flooding** olarak geçer.

Yukarıda anlatılan topolojilere göre şu şekilde çıkarımlarda bulunabiliriz

- Snifferlar ağ topolojisi ile sınırlıdırlar
  - Normal ağ sınırları dışına erişemezler
  - router, switch ötesini dinleyemezler
- Eğer paket snifferı ağ omurgasına koyarsanız intranetler arasındaki trafiği görebilirsiniz

3. Paket dinleme Metodları

Genel olarak üç türlü paket dinleme metodu vardır. Bunların bazıları shared ethernet ortamında bazıları ise switched ethernet ortamında da çalışmaktadır. Bu metodlar IP-temmeli, MAC-temelli ve ARP-temelli.

3.1 IP-temelli paket dinleme

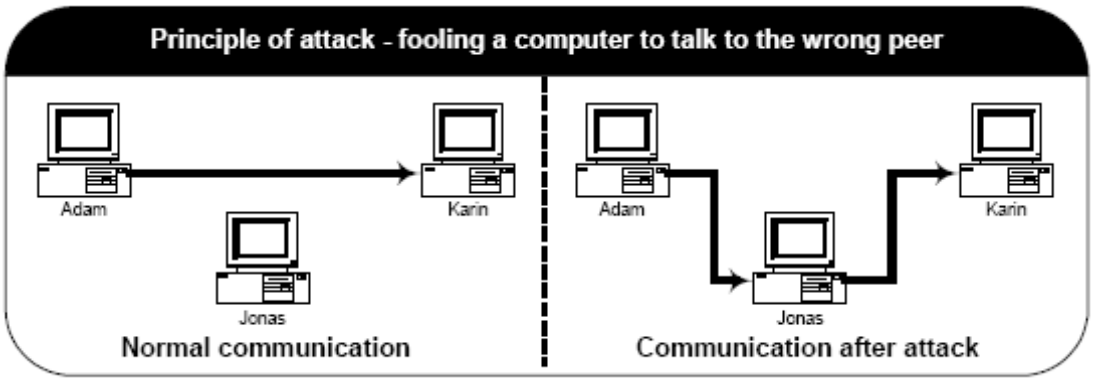
Paket dinlemek için en bilinen metottur. Ağ kartının promiscuous moda koyarak gelen bütün paketleri IP adreslerine göre toplamaktan ibarettir eğer IP adresine göre filtreleme yapmazsak bütün trafiği toplarız. Bu metod switch olmayan ağlarda çalışmaktadır

3.2 MAC- temelli paket dinleme

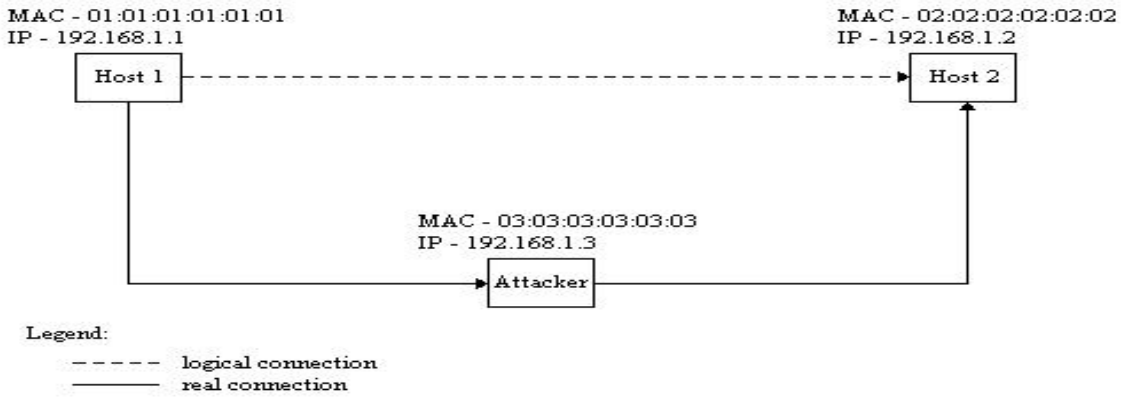
Bu metodta önceki metod gibi ağ kartını moda koyarak gelen bütün paketleri MAC adreslerine göre toplamaktan ibarettir. Bu metotta switch olmayan ağlardaçalışmaktadır

3.3 ARP-based sniffing

Bu metod yukarıda anlatılan ik metottan farklı çalışmaktadır bunun için ağ kartını promiscuous moda almaya gerek yoktur.Bu gerekli değildir çünkü Arp paketleri bize gönderilecektir. Bu durum ARP prorokolunün durumsuz olmasından kaynaklanır. Böyle oluncada paket dinlemeti switchli ortamlarda da yapabilmekteyiz.
Buradaki paket dinleme metodunu yapabilmek için ilk olarak paketlerini dinlemek istediğiniz hostların ARP kayıtlarını zehirlemeniz gerekmektedir. Aşağıdaki örnek teki gibi Adam Karin ile konuşmaya çalışırken Jonas adlı kişi bi ikis arasındaki haberleşmeyi dinlemek istemektedir. Burada Jonas Adam'a ben Karin, Karin'ede ben Adam demektedir ve iletişimi kendi üzerinden devam ettirmektedir. Bu aynı zamanda Man-In-theMiddle atak olarakta bilinir



Şekil 5 Man in the middle

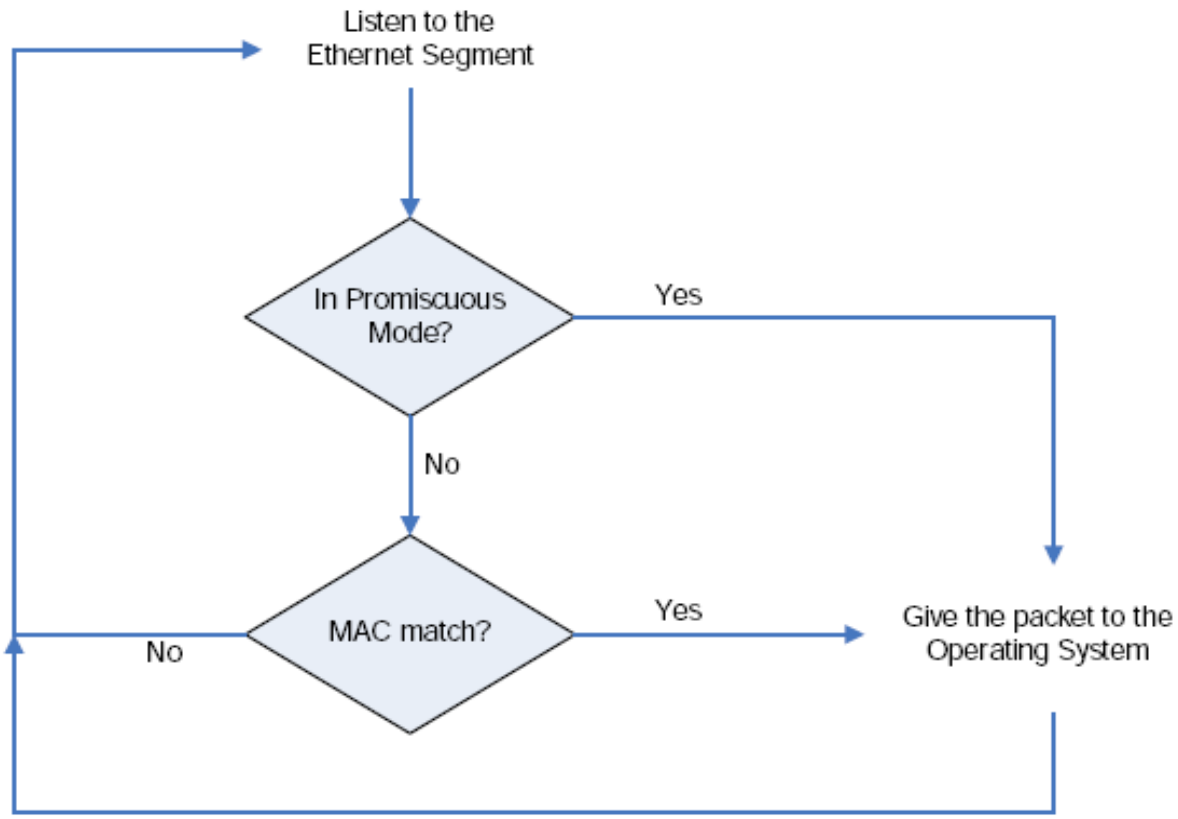


Şekil 6 Arp spoof

Görüldüğü gibi 192.168.1.1-01:01:01:01:01:01 ip-mac çiftine sahip Adam 02:02:02:02:02:02-192.168.1.2 mac-ip adresli Karin ile iletişime geçecektir.Normalde her iki host için Jonas kaydı 192.168.1.3-03:03:03:03:03:03 olarak bulunmaktadır burada Jonas,Adam -Karin ile iletişimi başlatmadan evvel Adam'a 192.168.1.2-02:02:02:02:02:02 adreslerinin kendisinde oldıuğunu söylemektedir ve Adam'da bu kaydı ARP cache'inde Jonas un soylediği şekilde saklamaktadır . Aynı şekilde Jonas, Karin'e 192.168.1.1-01:01:01:01:01:01 adresini saklması gerektiğini söyler ve yine bu kaydı Karin ARP cache inde saklar. Böylece trafik 192.168.1.1 den 192.168.1.2 ye doğru gitmektedir ama Jonas üzerinde geçerek gitmektedir. [8]

4.Paket dinlemeyi Tesbit etme

Paket dinleyicilerin nasıl çalıştığını anlatmaya çalıştık. Şimdide paket dinleyiciler nasıl tesbit edilir onlar hakkında bir kaç bir şey anlatalım.
Öncelikle paket dinleyicilerin bir çoğunun promiscuous mod da çalışması belirleyici bir özellik olacaktır aşağıdaki şekil gelen paketlere ethernet kartının nasıl davrandığını göstermektedir.



Şekil 7 Promiscuous mode

Görüldüğü gibi eğer ağ arayüz kartı promiscuous modda ise paketi işletim sistemine ulaştırmaktadır. Diğer türlü paket promiscuous modda değil ise bu defa MAC adresi makinanın MAC adresine eşit olup olmadığına yada paketin multicast yada broadcast paketi olduğuna bakılır bunlarada

uyuyorsa paket işletim sistemine teslim edilir. Diğer Türlü MAC adresi filtreleme mekanizmasına uymuyorsa paketle ilgilenilmez.

Varolan paket dinleyicilerin tesbiti

- Local host seviyesine belirleme (host-based)
- Local Network Segment seviyesinde belirleme (Network-based)

diye iki ana grupta toplayabiliriz.
yada

- Mac tabanlı Sniffing Belirleme
- Tuzağa düsürme yada aldatma tabanlı paket dinleyici belirleme

olarakta ikiye ayırabiliriz

Bunları teker teker açıklamak gerekirse

4.1 Local host seviyesine belirleme (host-based)

Literatüre bakaraktan birçok paket dinleyicinin UNIX üzerinde olduğunu söyleyebiliriz. Buna göre ağ arayüz kartının promiscuous modda olup olmadığını ifconfig çıktısına göre belirleyebiliriz. Aslında bu yöntem pekte mantıklı bir yöntem değildir. Çünkü sisteme atak yapan birisi bu programı değiştirmiş olabilir. Bu defa ifconfig çıktısı pekde güvenli olmamaktadır. Burada ethernet kartının promiscuous modda olup olmadığını çeşitli araçlarla öğrenebilirsiniz. neped.c yada cpm (check promiscuous mode) [9] bunlardan sadece ikisi...
promiscuous mod da olmayan hostun ifconfig çıktısı

```
 ifconfig
eth0    Link encap:Ethernet HWaddr 52:54:05:F3:95:01 inet
addr:203.199.66.243 Bcast:203.199. ... UP BROADCAST RUNNING MULTICAST
MTU:1500
```

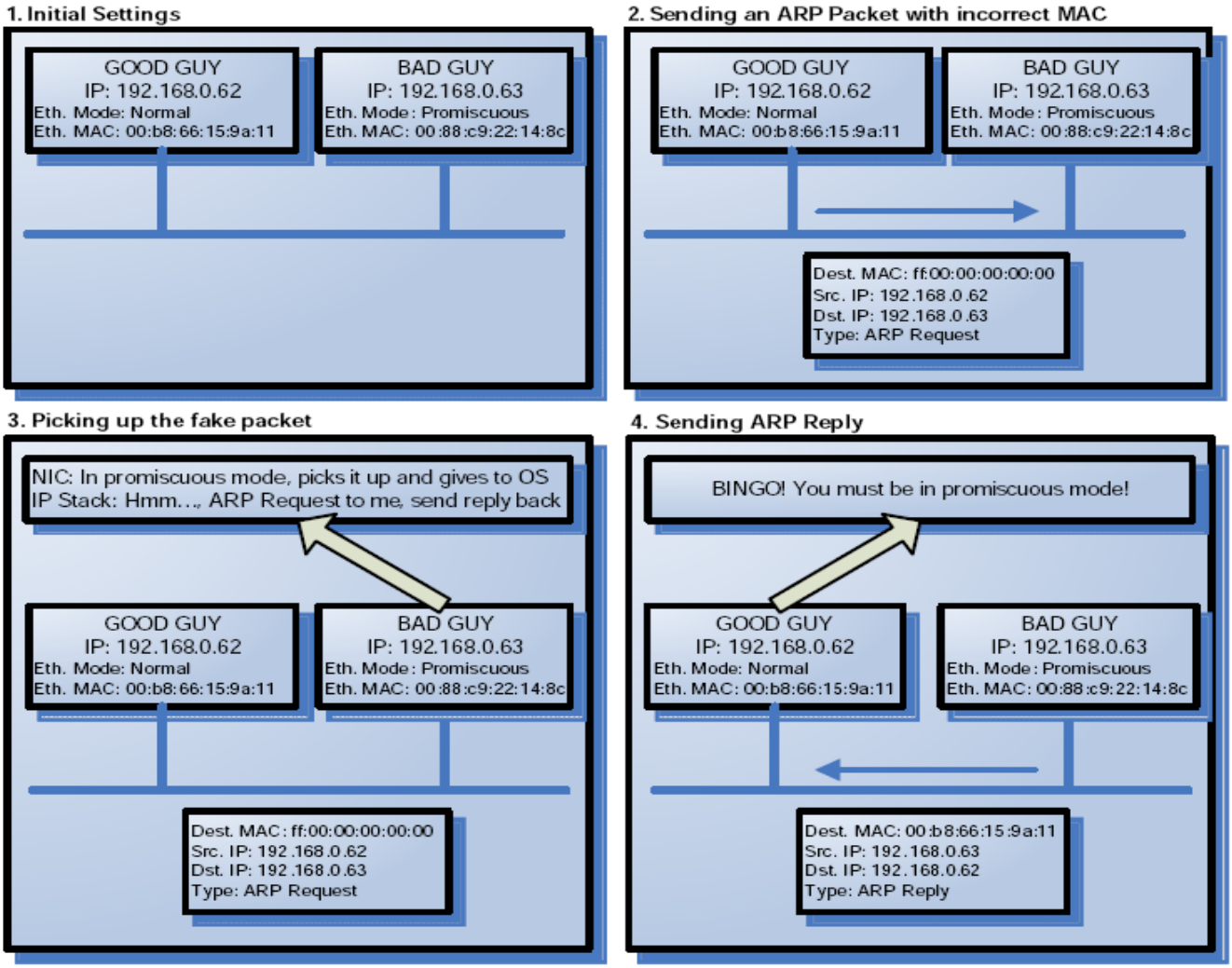
promiscuous mod da olan hostun ifconfig çıktısı

```
 ifconfig
eth0    Link encap:Ethernet HWaddr 52:54:05:F3:95:01 inet
addr:203.199.66.243 Bcast:203.199. ... UP BROADCAST RUNNING PROMISC
MULTICAST MTU:1500
```

4.2. MAC tabanlı Paket dinlemeyi belirleme

4.2.1 Arp metodu

Eğer ARP paketlerini hedef adres olarak broadcast adresi belirtmezsek ve bu paketi ağdaki herbir host a gönderirsek ve pakete yanıt alırsak yanıt aldığımız yanıtdaki makina promiscuous moddadır. Biraz daha açıklamak gerekirse ARP protokolü ile ulaşmaya çalıştığımız IP ait MAC adresini broadcast mesajı olarak yollar. diğeri hostlar ise bu gelen broadcast mesajına bakar ve arp sorgusu yapılan makina kendi cacheinde varsa MAC adres bilgisini arp reply mesajı olarak gönderir. Burada biz broadcast değilde unicast olarak arp request paketi gönderirsek sadece promiscuous mod da olan makina cevap verecektir. Aşağıdaki şekilde durum daha iyi anlaşılmaktadır.



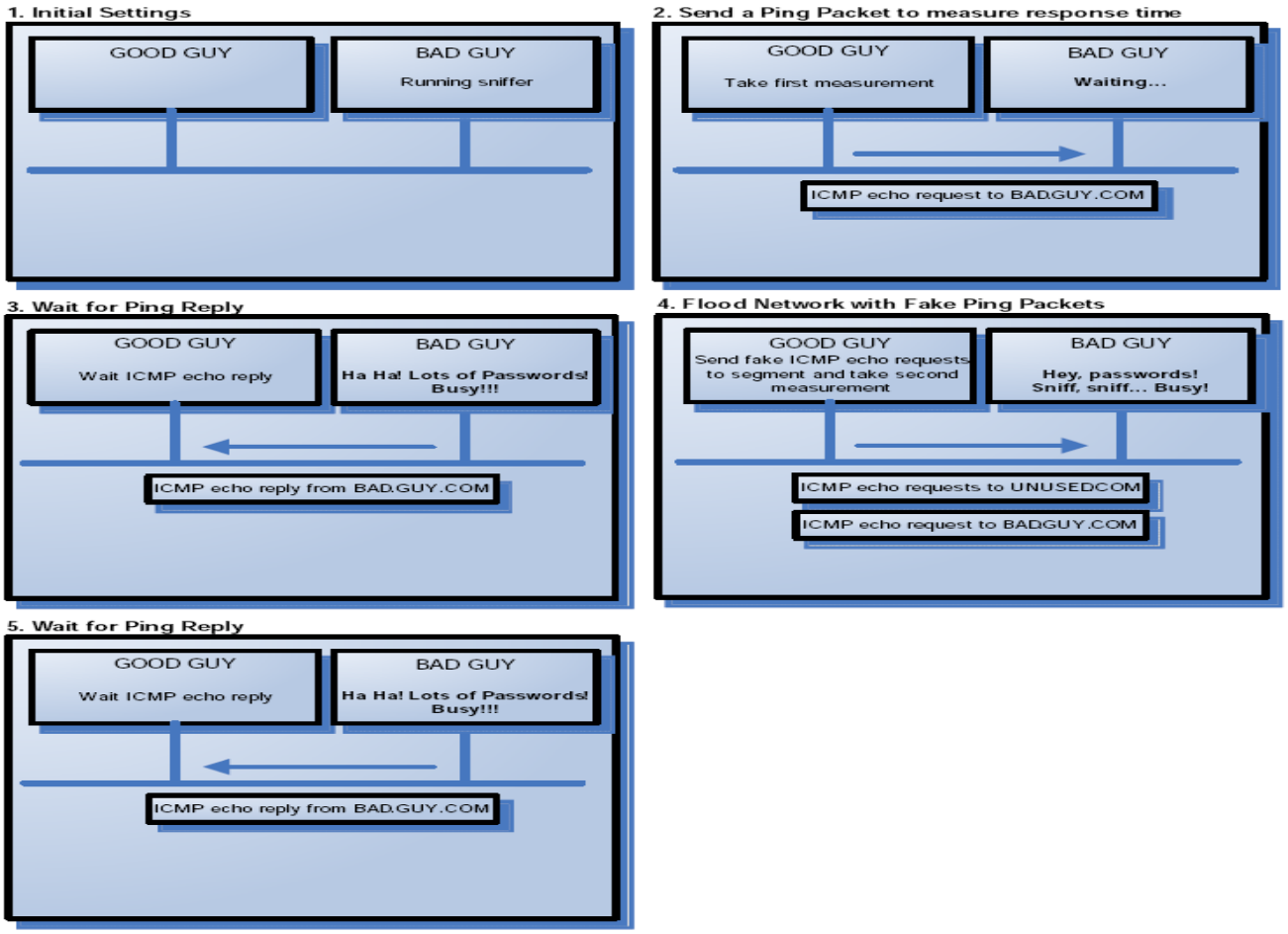
Şekil 8 Arp metodu

4.2.2 ARP Watch

Switchli ağlarda sniff yapabilmek için gateway in ARP spoof la dinleyebiliyorduk arpwatch benzeri arp cacheini takib eden yazılımlarla bir makina için birden fazla kayıt olup olmadığını görebiliriz. Eğer böyle birşey varsa bu makina için sniffer kullanıyor diyebiliriz. Ancak DHCP ile IP atanıyorsa bu yöntem hatalı sonuçlar doğuracaktır. Çünkü MAC-IP eşleşmeleri DHCP lease time sonrasında değişecektir. Basit bir değişikle bu hataları sayısını azaltabiliriz Buda DHCP lease time değerini artırarak olacaktır. [2]

4.2.3 Gecikme süresi Metodu

Bu yöntem şu varsayım üzerine kurulmuştur. Snifferlar topladıkları veriyi öncelikle parse edip işlerine yarayan verileri kaydetmektedirler.[3] Şimdi böyle bir durumda ufak bir ping testi yaparak makinanin şüpheli bir makina olup olmadığına bakabiliriz. Öncelikle makina pinglenir ardında çok büyük veri içeren paketler ağa gönderilir ve makina yine pinglenir. Eğer makina promiscuous modda isebütün paketleri ayrıştıracaktır ve buda makinanın aşırı yüklenmesine sebep olacaktır Sonraki pinge vereceği cevap için fazladan süre gerekecektir. İlk ping ve ikinci pinge verilen cevap süreleri makinanın promiscuous modda olup olmadığı hakkında fikir verecektir Burada aşırı paketlerden dolayı ping paketlerin gecikmeyeceği [1]



Şekil 9 Gecikme süresi metodu

4.2.4 IDS kullanma

Nüfûz tesbit sistemleri ağdaki ARP Spoofing gözlemleyebilmektedir. Örneğin Open Source IDS Snort arp-spoof önişlemcisine sahiptir. Böylece spoof edilmiş ARP adreslerin kayıt edebilmektedir [7]

4.3 Aldatma metodu

Yem yada Aldatma metodu Honeypotların mantığıyla çalışmaktadır. Temel fikir bir araç kullanarak sniffer olması muhtemel kişiyi (cezbederek) aldatmaya zorlamaktan ibarettir. Bu yanlış şifre yada yanlış kullanıcı adı ile olabilir. Böylece sniffer sahip olan kişi doğru sandığı bu bilgileri kullanarak saldırı yapabilir. Tabi burada sadece sniff işlemini yapan kişinin bu kullanıcı adı ve şifreyi kullanacağınıfarz ediyoruz. Şöyle bir senaryo sunarsak

Öncelikle Bir ftp server kurup root - admin - CIO gibi bir kullanıcı açalım. Daha sonra bu bilgilerin içerdiği bi ftp session açalım tabi bu arada saldırıyı yapacak olan kişi bu bilgileri elde edecek. Bu makinanın güvenlik önlemlerini iyi aldıktan sonra ayrıca birde bu oluşturulan sahte isim ve parola ile giriş yapanlar tesbit edilebilir bir mekanizma kuralım. Bu kullanıcı adını ve passwordu kullanan host tesbit edilir ve bu makina üzerinde paket dinleyici olduğu sonucuna varılabilir.

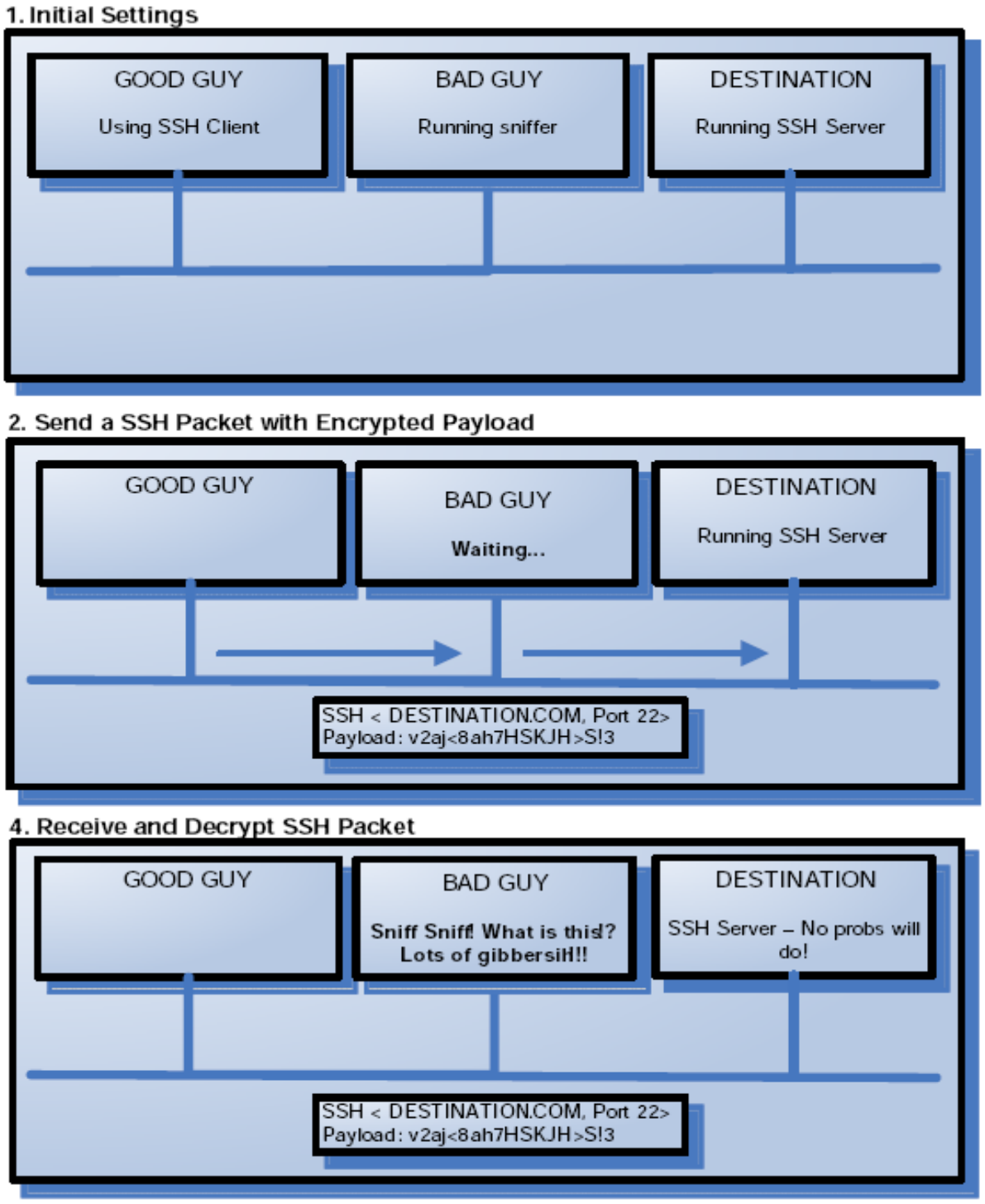
5. Trafik analizine Engel olma

5.1 Şifreleme :

Şifreleme ağ trafiğinden veri elde etmeye karşı en iyi yöntemdir. Bu bağlamda kullanılabilecek yöntemler şunlardır.

- SSH
  - SSH tunnel
- Web uygulamaları için SSL
- PGP mail
- IPSec
- VPN

Aşağıdaki şekilde başka bir makinaya secure shell ile bağlanırken ağdaki paket dinleyicilerin bu paketleri ele geçirsebile içeriğini göremedikleri için işine yaramadığı anlatılmaktadır.



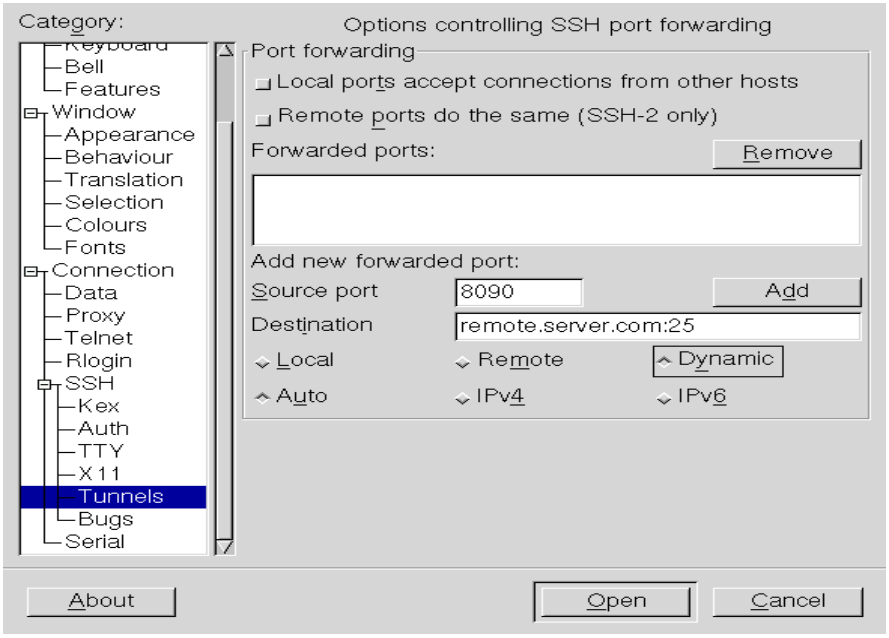
Şekil 10 ssh kullanımı

Uzaktaki sunuculara bağlanmak için kullandığımız ssh i kullanaraktan ortamdaki ağın güvenliğine güvenmiyorsak ağ trafiğimizi ssh tunel üzerinden geçirebiliriz. Bunu için

komut olarak

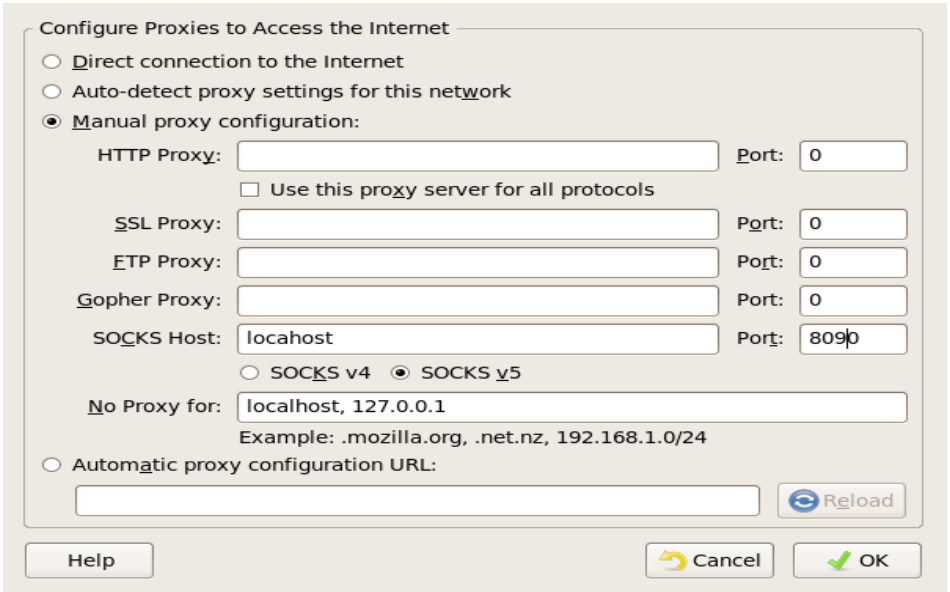
```
ssh  -f -C -D bizimPort -L PortNumarası:uzaktakisunucu:PortNumarası
```

kullanılabilir. Burada uzaktaki sunucunun PortNumarası ile bizimPort arasında tunel açmış bulunoruz ve bunu (-D) dinamik olarak gerçekleştiriyoruz. Yada ssh istemci olan putty kulanarak aşağıdaki şekilde yapabiliriz.



Şekil 11 putty

Ve bu tüneli kullanmak için Internet Explorer yada Firefox kullanımı...



Şekil 12 Proxy

6. Sonuç

Özellikle halka açık alanlarda plain text protokolleri kullanmamaya çalışın. Çünkü bu gibi ortamlarda SSH,HTTPS,POP3s,IMAPs veya tunnel (vpn veya ssh tunel) kullanılmadığı takdirde verilerimiz çok kolay bir şekilde paket dinleyicilerin eline geçmektedir.Anında Mesajlaşma MSN ICQ yerine Skype benzeri aynı zamanda şifreleme yapan programlar...

7. Kaynaklar

[1] AbdelallahElhadj, H., Khelalfa, H., & Kortebi, H. (2002). An Experimental Sniffer Detector: SnifferWall. Basic Software Laboratory, CERIST.

[2] Spangler, Ryan. (2003). Packet Sniffer Detection with AntiSniff. University of Wisconsin, Department of Computer and Network Administration.

[3] S. Grundschober. Sniffer Detector report. Diploma Thesis, IBM Research Division, Zurich Research

Laboratory, Global Security Analysis Lab, June 1998. http://packetstormsecurity.nl/

UNIX/IDS/grundschober_1998.letter.ps.gz.

[4] Butler, M., Postel, J., Chase, D., Goldberger, J., Reynolds, J.K. (1985) 'Post Office Protocol: Version 2 Post Office Protocol: Version 2', RFC0937, available from Internet <http://www.ietf.org/rfc/rfc0937.txt>, (30 May 2001)

[5] Tanenbaum, A.S. (1996) Computer Networks, 3rd edition, Prentice Hall, New Jersey

[6] Graham, Robert. (2000). Sniffing (network wiretap, sniffer) FAQ. [online document online document 2004-03-01]. URL http://www.robertgraham.com/pubs/sniffing-faq.html

[7] B. Mukherjee, T.L. Heberlein, and K.N. Levitt. Network intrusion detection. IEEE Network, vol. 8, no.
3, pages 26–41, May/June 1994.

[8] D. Sumit , "Sniffers Basics and Detection " Information Security Management Team Reliance Infocomm ,December 2002

[9] CPM Check for network interfaces in Promiscuous Mode : ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/cpm

[10] Huzeyfe ÖNAL "Ag Trafigi Dinleme Ve Yorumlama" http://www.enderunix.org/slides/Linuxsenligi2006/sniff.pdf