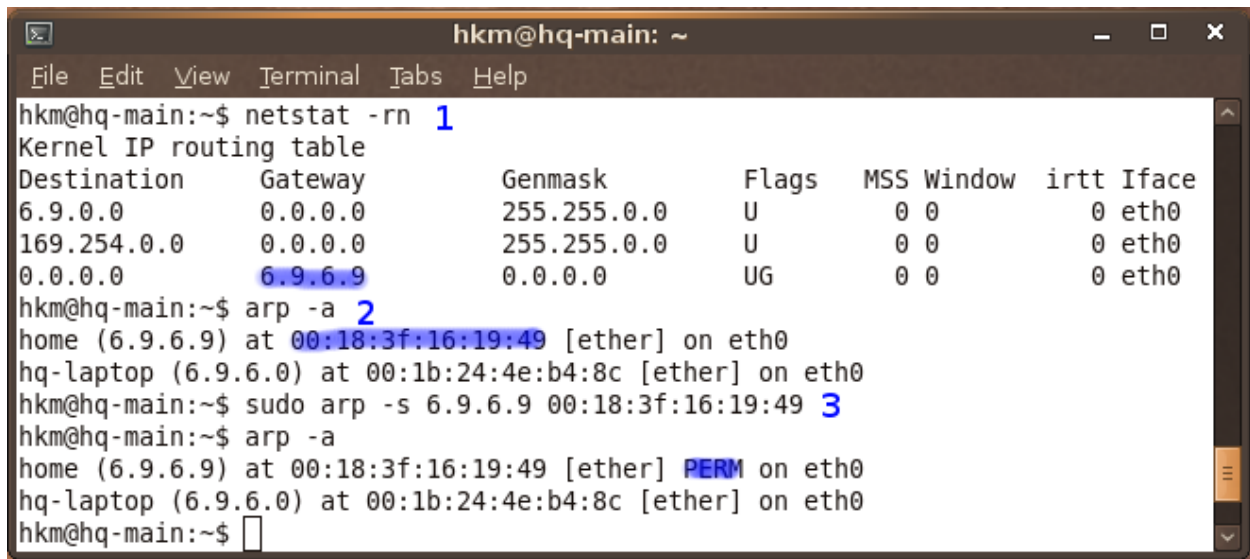


# Protección contra ARP Spoofing

Una guía multiplataforma.

Para **prevención de ARP Spoofing** se utilizarán los comandos **netstat** y **arp** ya que es el mismo procedimiento para la mayoría de sistemas operativos. La **detección** se llevará a cabo de forma manual con el comando **arp** y con el mejor sniffer multiplataforma **Wireshark**. La última sección cubre **monitoreo automatizado** en Windows usando **DecaffeinatID** y en Linux con **arpwatch**.

## Prevención de ARP Spoofing



```
hkm@hq-main: ~  
File Edit View Terminal Tabs Help  
hkm@hq-main:~$ netstat -rn 1  
Kernel IP routing table  
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface  
6.9.0.0          0.0.0.0         255.255.0.0    U        0  0        0 eth0  
169.254.0.0     0.0.0.0         255.255.0.0    U        0  0        0 eth0  
0.0.0.0         6.9.6.9         0.0.0.0        UG       0  0        0 eth0  
hkm@hq-main:~$ arp -a 2  
home (6.9.6.9) at 00:18:3f:16:19:49 [ether] on eth0  
hq-laptop (6.9.6.0) at 00:1b:24:4e:b4:8c [ether] on eth0  
hkm@hq-main:~$ sudo arp -s 6.9.6.9 00:18:3f:16:19:49 3  
hkm@hq-main:~$ arp -a  
home (6.9.6.9) at 00:18:3f:16:19:49 [ether] PERM on eth0  
hq-laptop (6.9.6.0) at 00:1b:24:4e:b4:8c [ether] on eth0  
hkm@hq-main:~$
```

Paso 1: Obtenemos el IP del Gateway

### **netstat -rn**

Muestra en forma numérica la tabla de ruteo, hay una columna que muestra el IP del Gateway.

En el ejemplo el IP es 6.9.6.9.

Paso 2: Obtenemos la dirección MAC del Gateway

### **arp -a**

Lista la tabla ARP, buscamos el IP del Gateway y a un lado tendremos su MAC.

En el ejemplo 6.9.6.9 tiene MAC 00:18:3f:16:19:49.

Hacer esto cuando se este seguro que no nos están atacando y que el MAC si es el original.

Paso 3:

### **arp -s <IP> <MAC>**

Agrega una entrada estática a la tabla ARP.

Podemos comprobar que se ha puesto una entrada estática si listamos de nuevo la tabla con

**arp -a** y podemos observar que hay una entrada **PERManente**.

Para borrar esa entrada permanente utilizamos el comando **arp -d <IP>**

En **Windows** lo único que cambia es el formato los comandos y el procedimiento es exactamente el mismo:

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\r68fyi>netstat -rn

Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x10003 ...08 00 27 f7 ce 88 ..... AMD PCNET Family Ethernet Adapter (PCI) - Pa
cket Scheduler Miniport
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          10.0.2.2         10.0.2.15        20
10.0.2.0               255.255.255.0   10.0.2.15       10.0.2.15        20
10.0.2.15             255.255.255.255 127.0.0.1       127.0.0.1        20
10.255.255.255        255.255.255.255 10.0.2.15       10.0.2.15        20
127.0.0.0             255.0.0.0       127.0.0.1       127.0.0.1        1
224.0.0.0             240.0.0.0       10.0.2.15       10.0.2.15        20
255.255.255.255      255.255.255.255 10.0.2.15       10.0.2.15        1
Default Gateway:      10.0.2.2
=====
Persistent Routes:
None

C:\Documents and Settings\r68fyi>arp -a

Interface: 10.0.2.15 --- 0x10003
Internet Address      Physical Address      Type
10.0.2.3             52-54-00-12-35-03    dynamic

C:\Documents and Settings\r68fyi>ping 10.0.2.2

Pinging 10.0.2.2 with 32 bytes of data:

Reply from 10.0.2.2: bytes=32 time=1ms TTL=255

Ping statistics for 10.0.2.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C
C:\Documents and Settings\r68fyi>arp -a

Interface: 10.0.2.15 --- 0x10003
Internet Address      Physical Address      Type
10.0.2.2             52-54-00-12-35-02    dynamic
10.0.2.3             52-54-00-12-35-03    dynamic

C:\Documents and Settings\r68fyi>arp -s 10.0.2.2 52-54-00-12-35-02

C:\Documents and Settings\r68fyi>arp -a

Interface: 10.0.2.15 --- 0x10003
Internet Address      Physical Address      Type
10.0.2.2             52-54-00-12-35-02    static
10.0.2.3             52-54-00-12-35-03    dynamic

C:\Documents and Settings\r68fyi>
```

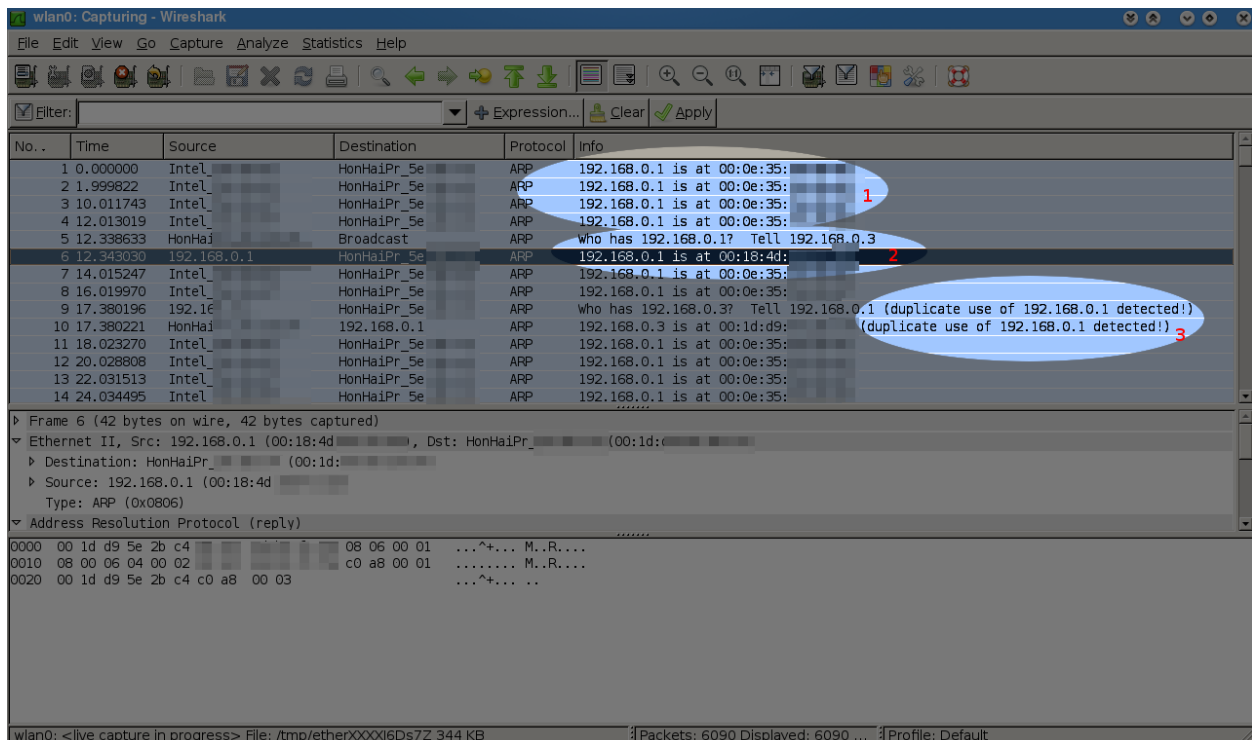
En este caso como no teníamos el gateway en la tabla arp utilizamos **ping <IP>** para resolverlo y que se agregue automáticamente a la tabla

## Detección de ARP Spoofing

Tan sencillo como verificar que la MAC listada en **arp -a** sea la MAC verdadera de nuestro Gateway. Para obtener el MAC autentico del Gateway debemos seguir los pasos 1 y 2 explicados anteriormente, cuando estemos seguros de que no estamos siendo atacados. Es por eso que recomiendo **tener una lista de direcciones MAC autenticas** del Gateway de los lugares donde creamos que podamos ser víctima de ARP Spoofing, ej. casa, oficina, café internet, etc.

**Wireshark** <http://www.wireshark.org>

Wireshark es un sniffer que corre en los tres sistemas operativos y tiene, entre sus múltiples funciones, la detección de ARP Spoofing



Podemos agregar como Filtro: **arp** y observar las siguientes características en el trafico:

- 1 Un host esta anunciando su MAC sin que otros hosts se lo pidan
- 2 Un host solicita la MAC y hay dos respuestas de la misma IP con MAC diferente
- 3 Wireshark detecta el spoof: "**duplicate use of <IP> detected!**"

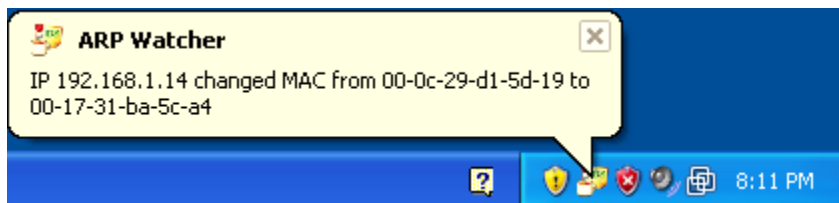
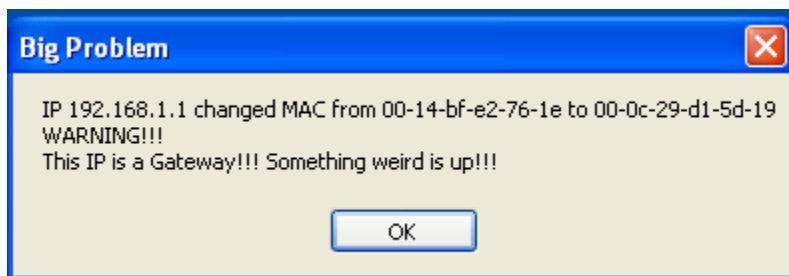
## Monitoreo automatizado de ARP Spoofing

Para el monitoreo automático es necesario diferentes programas para diferentes sistemas operativos solo nombrare los que a mi me parecen interesantes. **No son los mejores, los mejores podrían ser un Snort o algun otro IDS bien configurado.**

### [WINDOWS]

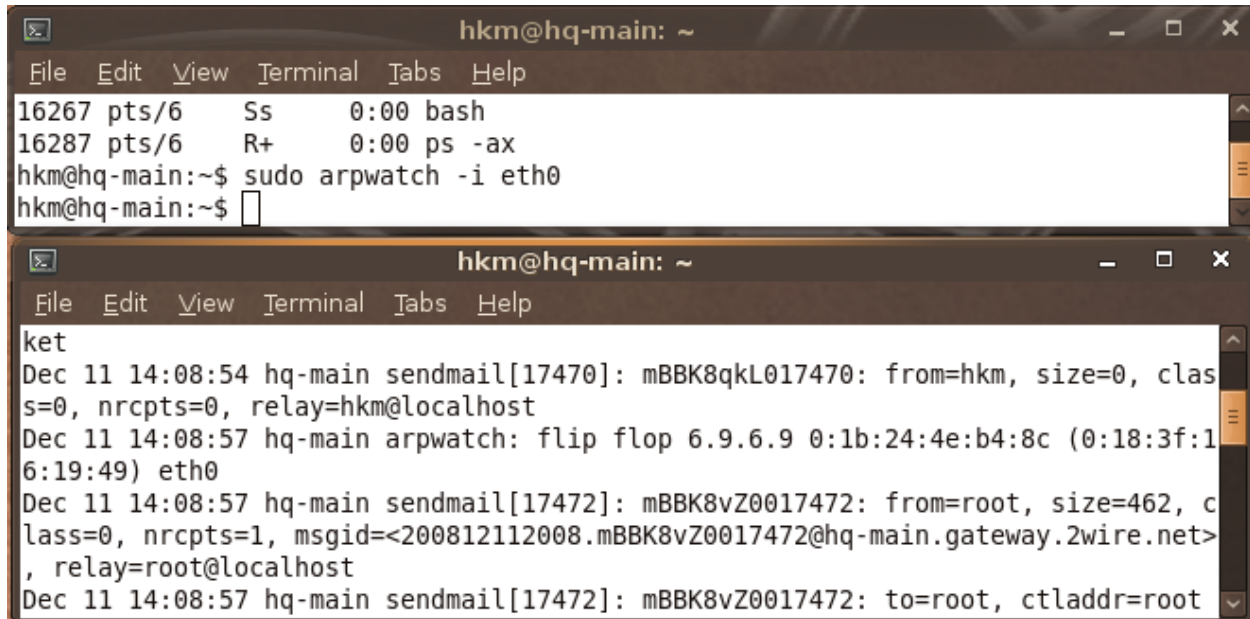
**DecaffeinatID** <http://www.irongeek.com/i.php?page=security/decaffeinatid-simple-ids-arpwatch-for-windows>

DecaffeinatID es un programa hecho en AutoIT por IronGeek (<http://www.irongeek.com>) funciona en Windows XP y Vista. Esta constantemente checando los Event y Firewall logs y te alerta cuando hay un cambio del MAC del Gateway.



### [LINUX]

**Arpwatch** fue publicado en el 2003 por LBL Research Group (<http://www.lbl.gov/>) usa libpcap y monitorea cambios en las relaciones de IP - MAC. Alerta via correo y con mensajes en los logs.



```
hkm@hq-main: ~  
File Edit View Terminal Tabs Help  
16267 pts/6 Ss 0:00 bash  
16287 pts/6 R+ 0:00 ps -ax  
hkm@hq-main:~$ sudo arpwatc -i eth0  
hkm@hq-main:~$  
  
hkm@hq-main: ~  
File Edit View Terminal Tabs Help  
ket  
Dec 11 14:08:54 hq-main sendmail[17470]: mBBK8qkL017470: from=hkm, size=0, class=0, nrcpts=0, relay=hkm@localhost  
Dec 11 14:08:57 hq-main arpwatc: flip flop 6.9.6.9 0:1b:24:4e:b4:8c (0:18:3f:16:19:49) eth0  
Dec 11 14:08:57 hq-main sendmail[17472]: mBBK8vZ0017472: from=root, size=462, class=0, nrcpts=1, msgid=<200812112008.mBBK8vZ0017472@hq-main.gateway.2wire.net>, relay=root@localhost  
Dec 11 14:08:57 hq-main sendmail[17472]: mBBK8vZ0017472: to=root, ctladdr=root
```

### **sudo arpwatc -i <INTERFACE>**

Este comando no regresa nada, pero cuando un cambio en MAC/IP es detectado, muestra un mensaje en el /var/log/syslog (o /var/log/message).

### **tail -f /var/log/syslog**

Con este comando monitoreamos el final del /var/log/syslog.

En este ejemplo observamos como el arpwatc manda una alerta por correo con sendmail.

### **REFERENCIAS:**

How do I check the default gateway on an unix/linux machine

<http://www.dslreports.com/forum/r19287746-How-do-I-check-the-default-gateway-on-an-unixlinux-machine>

Detect and Counter ARP Poisoning under Windows and Linux

<http://linux-tips.blogspot.com/2008/06/detect-and-counter-arp-poisoning-under.html>

How to: Detect ARP Spoofing under UNIX or Linux

<http://www.cyberciti.biz/faq/how-to-detect-arp-spoofing-under-unix-or-linux/>

***www.hakim.ws***

**h k m @ h a k i m . w s**

11/12/2008