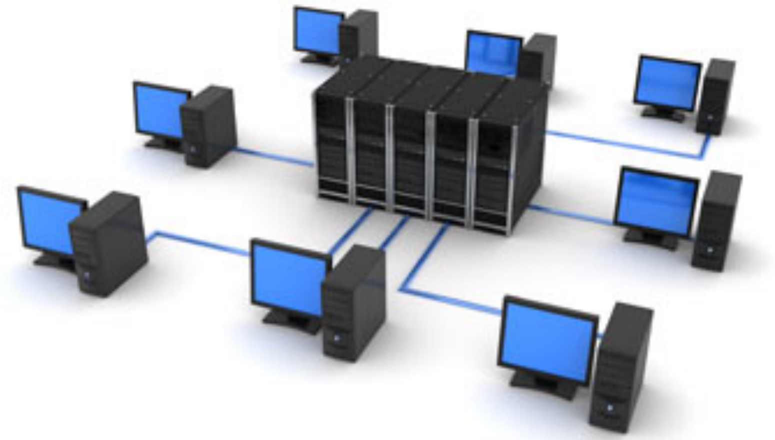
MAC FLOODING

OpenWebinars



***MAC Flooding* consiste en agotar la tabla de *MACs* de un dispositivo para provocar un envío a difusión**

1.

INTRODUCCIÓN

INTRODUCCIÓN

- Tablas MAC de tamaño limitado
- Switch relacionan *<MAC:Puerto>*
- Tabla MAC llena… ¿Por dónde lo envía?

“Broadcast”

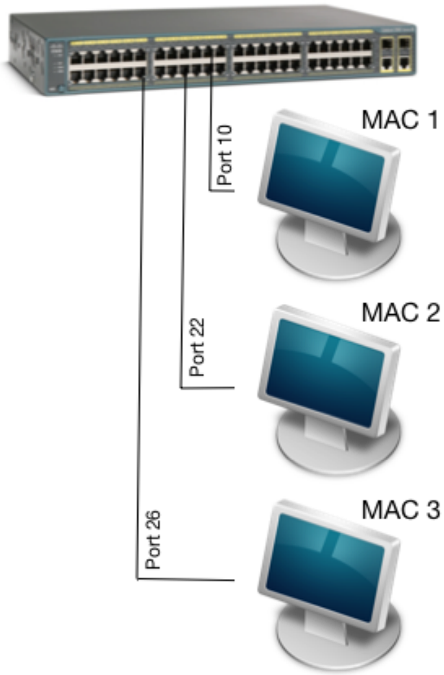
2.

SWITCH Y ATAQUE

FUNCIONAMIENTO SWITCH

- Crea una tabla con las relaciones

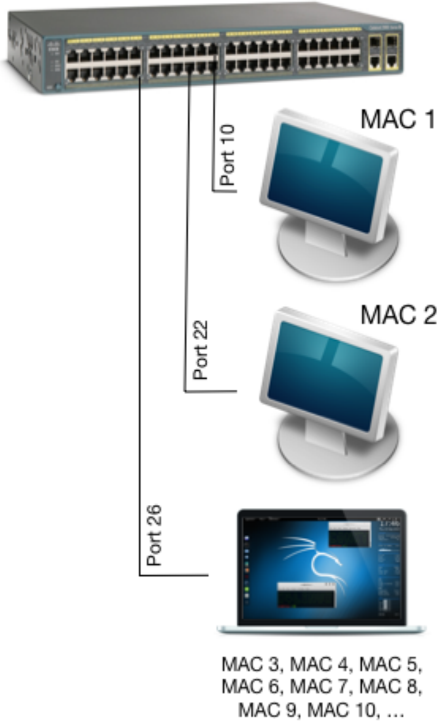
Nº	MAC	Puerto
1	MAC 1	10
2	MAC 2	22
3	MAC 3	26



MAC FLOODING

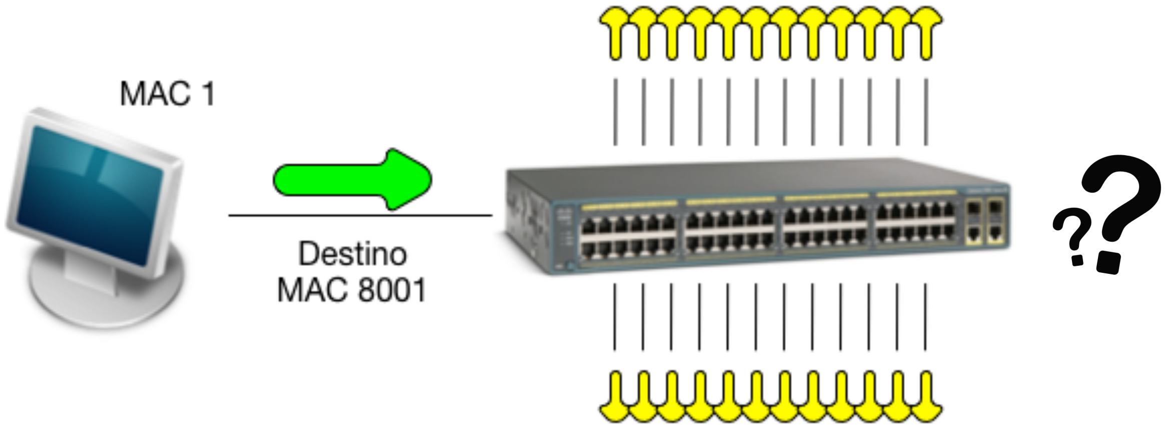
- Tabla llena

Nº	MAC	Puerto
…	…	…
7998	MAC 7998	26
7999	MAC 7999	26
8000	MAC 8000	26



CONSECUENCIA

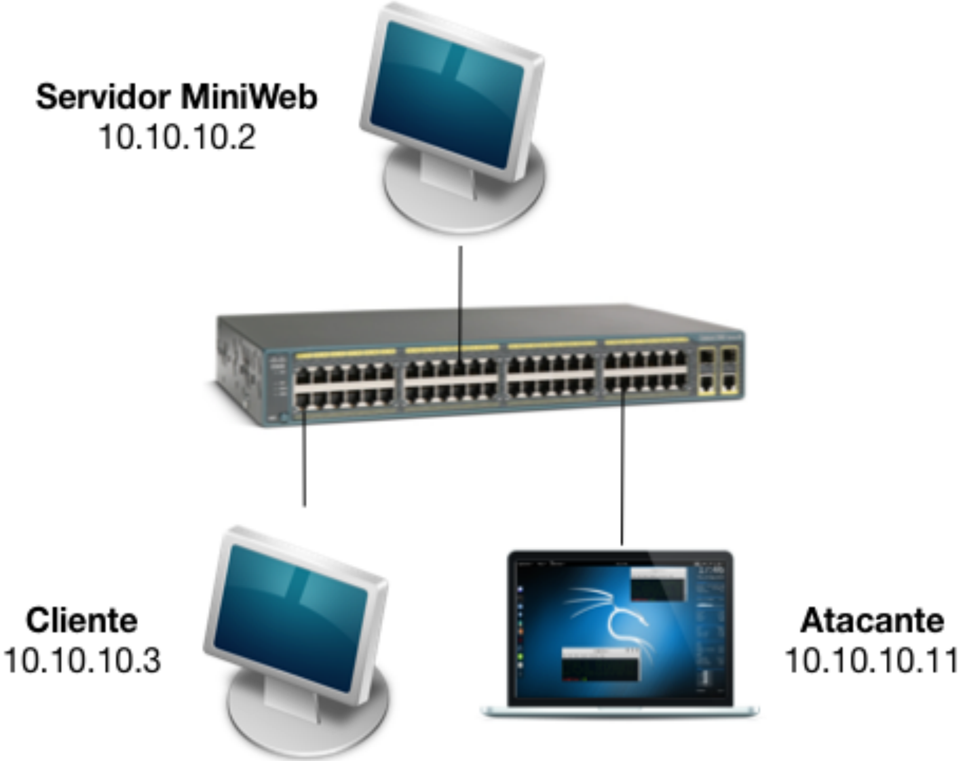
- Envío a difusión (Broadcast)
- Posibilidad de escuchar tráfico



3.

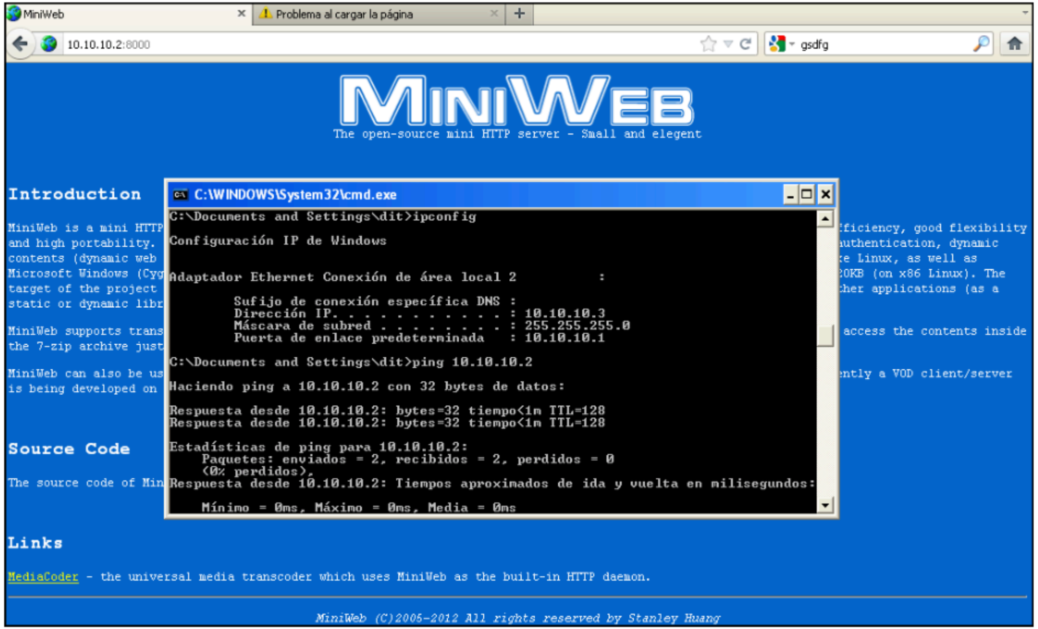
LABORATORIO

ESCENARIO


Servidor MiniWeb
10.10.10.2
Cliente
10.10.10.3
Atacante
10.10.10.11

MAC FLOODING

El cliente tiene acceso al *MiniWeb*



The open-source mini HTTP server - Small and elegent

Introduction

MiniWeb is a mini HTTP … ficiency, good flexibility
and high portability. … uthentication, dynamic
contents (dynamic web … e Linux, as well as
Microsoft Windows (Cyg … 0KB (on x86 Linux). The
target of the project … her applications (as a
static or dynamic libr

MiniWeb supports trans … access the contents inside
the 7-zip archive just

MiniWeb can also be us … ntly a VOD client/server
is being developed on

Source Code

The source code of Min

Links

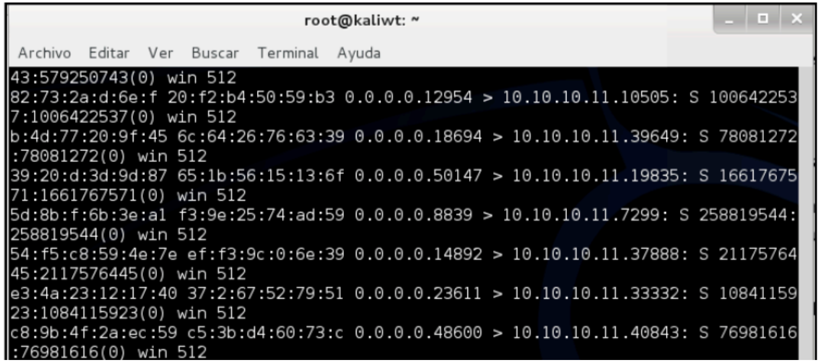
MediaCoder - the universal media transcoder which uses MiniWeb as the built-in HTTP daemon.

MiniWeb (C)2005-2012 All rights reserved by Stanley Huang

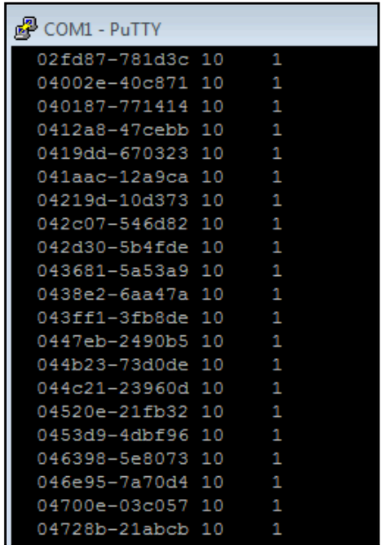
```
C:\Documents and Settings\dit>ipconfig

Configuración IP de Windows


Adaptador Ethernet Conexión de área local 2         :

        Sufijo de conexión específica DNS :
        Dirección IP. . . . . . . . . . . : 10.10.10.3
        Máscara de subred . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada   : 10.10.10.1

C:\Documents and Settings\dit>ping 10.10.10.2

Haciendo ping a 10.10.10.2 con 32 bytes de datos:

Respuesta desde 10.10.10.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.10.10.2: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.10.10.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Respuesta desde 10.10.10.2: Tiempos aproximados de ida y vuelta en milisegundos:

    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

MAC FLOODING

El atacante comienza la inundación de MAC



```
43:579250743(0) win 512
82:73:2a:d:6e:f 20:f2:b4:50:59:b3 0.0.0.0.12954 > 10.10.10.11.10505: S 100642253
7:1006422537(0) win 512
b:4d:77:20:9f:45 6c:64:26:76:63:39 0.0.0.0.18694 > 10.10.10.11.39649: S 78081272
:78081272(0) win 512
39:20:d:3d:9d:87 65:1b:56:15:13:6f 0.0.0.0.50147 > 10.10.10.11.19835: S 16617675
71:1661767571(0) win 512
5d:8b:f:6b:3e:a1 f3:9e:25:74:ad:59 0.0.0.0.8839 > 10.10.10.11.7299: S 258819544:
258819544(0) win 512
54:f5:c8:59:4e:7e ef:f3:9c:0:6e:39 0.0.0.0.14892 > 10.10.10.11.37888: S 21175764
45:2117576445(0) win 512
e3:4a:23:12:17:40 37:2:67:52:79:51 0.0.0.0.23611 > 10.10.10.11.33332: S 10841159
23:1084115923(0) win 512
c8:9b:4f:2a:ec:59 c5:3b:d4:60:73:c 0.0.0.0.48600 > 10.10.10.11.40843: S 76981616
:76981616(0) win 512
```

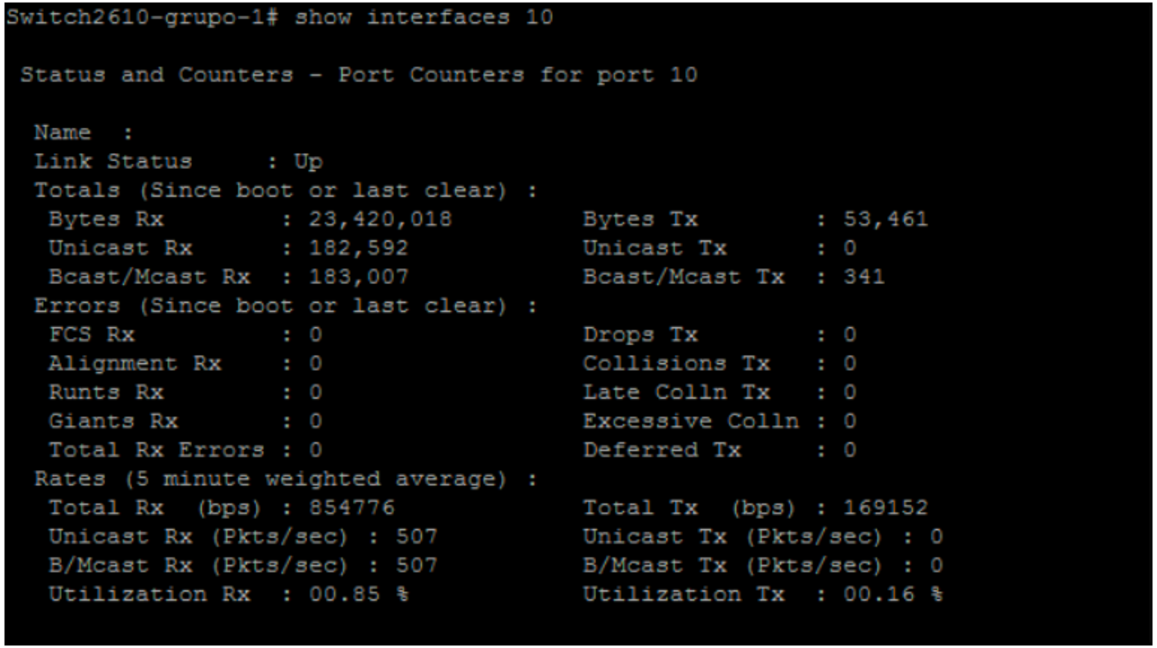


```
  02fd87-781d3c 10      1
  04002e-40c871 10      1
  040187-771414 10      1
  0412a8-47cebb 10      1
  0419dd-670323 10      1
  041aac-12a9ca 10      1
  04219d-10d373 10      1
  042c07-546d82 10      1
  042d30-5b4fde 10      1
  043681-5a53a9 10      1
  0438e2-6aa47a 10      1
  043ff1-3fb8de 10      1
  0447eb-2490b5 10      1
  044b23-73d0de 10      1
  044c21-23960d 10      1
  04520e-21fb32 10      1
  0453d9-4dbf96 10      1
  046398-5e8073 10      1
  046e95-7a70d4 10      1
  04700e-03c057 10      1
  04728b-21abcb 10      1
```

Herramienta: ***macof*** de Kali

MAC FLOODING

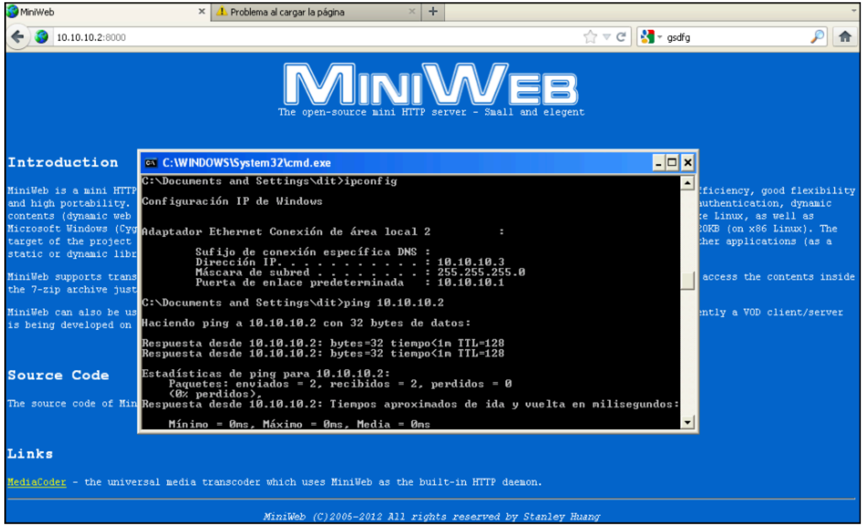
Tabla 8000 / 500 entradas/seg ≈ ***16 segundos***



```
Switch2610-grupo-1# show interfaces 10

 Status and Counters - Port Counters for port 10

  Name    :
  Link Status      : Up
  Totals (Since boot or last clear) :
   Bytes Rx         : 23,420,018          Bytes Tx          : 53,461
   Unicast Rx       : 182,592             Unicast Tx        : 0
   Bcast/Mcast Rx   : 183,007             Bcast/Mcast Tx    : 341
  Errors (Since boot or last clear) :
   FCS Rx           : 0                   Drops Tx          : 0
   Alignment Rx     : 0                   Collisions Tx     : 0
   Runts Rx         : 0                   Late Colln Tx     : 0
   Giants Rx        : 0                   Excessive Colln : 0
   Total Rx Errors : 0                    Deferred Tx       : 0
  Rates (5 minute weighted average) :
   Total Rx   (bps) : 854776              Total Tx   (bps) : 169152
   Unicast Rx (Pkts/sec) : 507            Unicast Tx (Pkts/sec) : 0
   B/Mcast Rx (Pkts/sec) : 507            B/Mcast Tx (Pkts/sec) : 0
   Utilization Rx  : 00.85 %              Utilization Tx  : 00.16 %
```

MAC FLOODING

El cliente accede al *MiniWeb* sin que el atacante vea nada



The open-source mini HTTP server - Small and elegent

Introduction

MiniWeb is a mini HTTP
and high portability.
contents (dynamic web
Microsoft Windows (Cyg
target of the project
static or dynamic libr

MiniWeb supports trans
the 7-zip archive just

MiniWeb can also be us
is being developed on

ficiency, good flexibility
authentication, dynamic
e Linux, as well as
0KB (on x86 Linux). The
ther applications (as a

access the contents inside

ntly a VOD client/server

Source Code

The source code of Min

```
C:\Documents and Settings\dit>ipconfig

Configuración IP de Windows


Adaptador Ethernet Conexión de área local 2          :

        Sufijo de conexión específica DNS :
        Dirección IP. . . . . . . . . . . : 10.10.10.3
        Máscara de subred . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada   : 10.10.10.1

C:\Documents and Settings\dit>ping 10.10.10.2

Haciendo ping a 10.10.10.2 con 32 bytes de datos:

Respuesta desde 10.10.10.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.10.10.2: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.10.10.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Respuesta desde 10.10.10.2: Tiempos aproximados de ida y vuelta en milisegundos:

    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

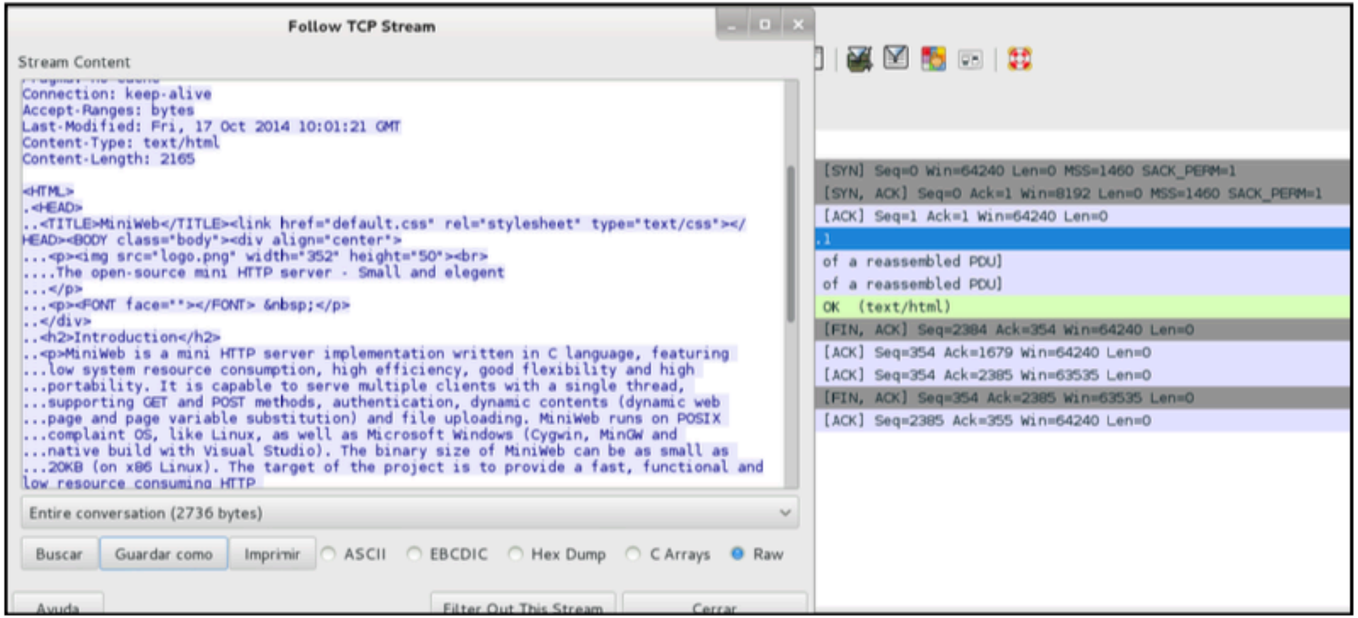
Links

MediaCoder - the universal media transcoder which uses MiniWeb as the built-in HTTP daemon.

MiniWeb (C)2005-2012 All rights reserved by Stanley Huang

MAC FLOODING

Limpieza de la tabla: *clear mac-address vlan 1*



Follow TCP Stream

Stream Content

```
Connection: keep-alive
Accept-Ranges: bytes
Last-Modified: Fri, 17 Oct 2014 10:01:21 GMT
Content-Type: text/html
Content-Length: 2165

<HTML>
.<HEAD>
..<TITLE>MiniWeb</TITLE><link href="default.css" rel="stylesheet" type="text/css"></
HEAD><BODY class="body"><div align="center">
...<p><img src="logo.png" width="352" height="50"><br>
....The open-source mini HTTP server - Small and elegent
...</p>
...<p><FONT face=""></FONT> &nbsp;</p>
..</div>
..<h2>Introduction</h2>
..<p>MiniWeb is a mini HTTP server implementation written in C language, featuring
...low system resource consumption, high efficiency, good flexibility and high
...portability. It is capable to serve multiple clients with a single thread,
...supporting GET and POST methods, authentication, dynamic contents (dynamic web
...page and page variable substitution) and file uploading. MiniWeb runs on POSIX
...complaint OS, like Linux, as well as Microsoft Windows (Cygwin, MinGW and
...native build with Visual Studio). The binary size of MiniWeb can be as small as
...20KB (on x86 Linux). The target of the project is to provide a fast, functional and
low resource consuming HTTP
```

Entire conversation (2736 bytes)

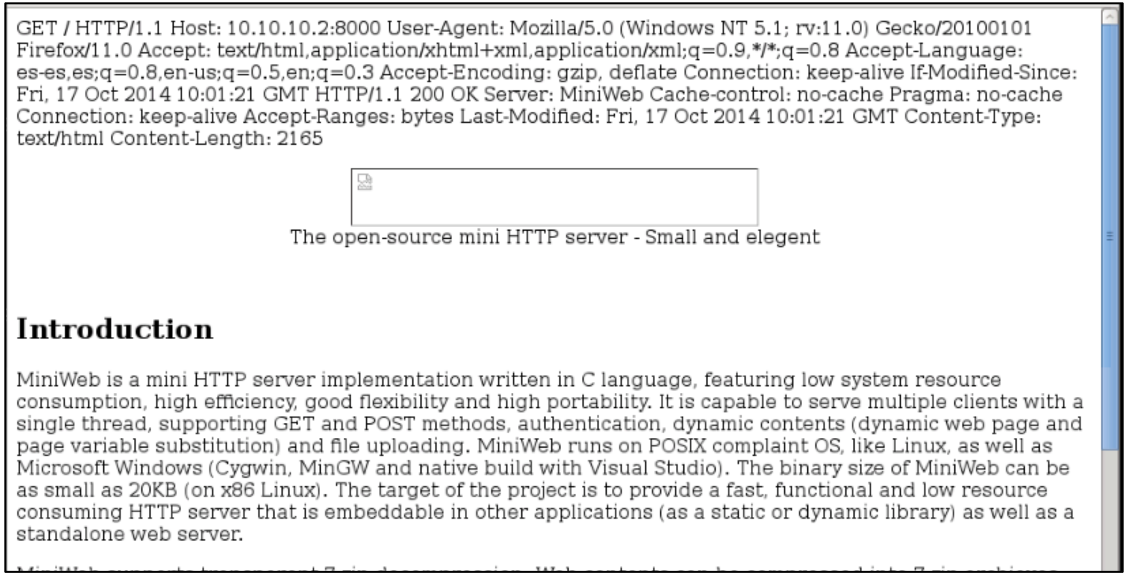
Buscar | Guardar como | Imprimir | ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Ayuda | Filter Out This Stream | Cerrar

```
[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
[ACK] Seq=1 Ack=1 Win=64240 Len=0
.1
of a reassembled PDU]
of a reassembled PDU]
OK  (text/html)
[FIN, ACK] Seq=2384 Ack=354 Win=64240 Len=0
[ACK] Seq=354 Ack=1679 Win=64240 Len=0
[ACK] Seq=354 Ack=2385 Win=63535 Len=0
[FIN, ACK] Seq=354 Ack=2385 Win=63535 Len=0
[ACK] Seq=2385 Ack=355 Win=64240 Len=0
```

MAC FLOODING

Tráfico a la vista del atacante



GET / HTTP/1.1 Host: 10.10.10.2:8000 User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko/20100101 Firefox/11.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: es-es,es;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Connection: keep-alive If-Modified-Since: Fri, 17 Oct 2014 10:01:21 GMT HTTP/1.1 200 OK Server: MiniWeb Cache-control: no-cache Pragma: no-cache Connection: keep-alive Accept-Ranges: bytes Last-Modified: Fri, 17 Oct 2014 10:01:21 GMT Content-Type: text/html Content-Length: 2165

The open-source mini HTTP server - Small and elegent

Introduction

MiniWeb is a mini HTTP server implementation written in C language, featuring low system resource consumption, high efficiency, good flexibility and high portability. It is capable to serve multiple clients with a single thread, supporting GET and POST methods, authentication, dynamic contents (dynamic web page and page variable substitution) and file uploading. MiniWeb runs on POSIX complaint OS, like Linux, as well as Microsoft Windows (Cygwin, MinGW and native build with Visual Studio). The binary size of MiniWeb can be as small as 20KB (on x86 Linux). The target of the project is to provide a fast, functional and low resource consuming HTTP server that is embeddable in other applications (as a static or dynamic library) as well as a standalone web server.

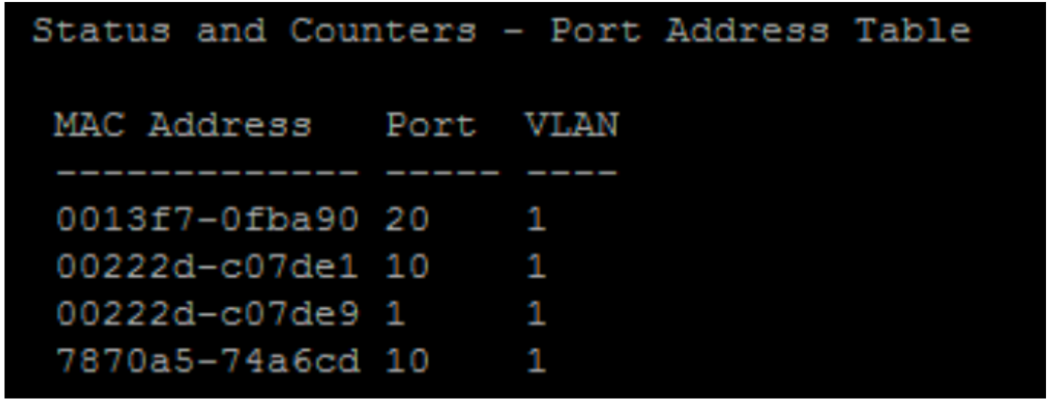
4.

PREVENCIÓN

MAC FLOODING

Limitar MACs por puerto

# port-security 10 address-limit 2 learn-mode limited-continuous



```
Status and Counters - Port Address Table

 MAC Address   Port  VLAN
 ------------- ----- ----
 0013f7-0fba90 20    1
 00222d-c07de1 10    1
 00222d-c07de9 1     1
 7870a5-74a6cd 10    1
```