

Índice:

Ejercicio 1	2
a) Barrido de ping.....	2
b) Visualizar puertos abiertos del equipo atacado.....	3
c) Captura los paquetes de la red.....	4
d) Cerrar y abrir puertos en Linux y Windows	5
e) Para detectar sniffers.....	8

Ejercicio 3

a) Barrido de ping

Solución:

IP del equipo Windows (Equipo amenazado)

Win10_SRI [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

```
Simbolo del sistema
Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.168.60.43
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.60.254

C:\Users\Usuario>
```

Miguelillo

Escaneamos con nmap -A 192.168.60.0/24

Se puede ver que detecta que es un equipo Windows

```
ricardo@ricardo-VirtualBox:~$ nmap -A 192.168.60.0/24

Nmap scan report for 192.168.60.43
Host is up (0.28s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Service Unavailable
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: 1s
|_ nbstat: NetBIOS name: DESKTOP-7PEK6DG, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:e9:46:37 (Oracle VirtualBox virtual NIC)
|_ smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2023-09-26T07:58:43
|_ start_date: N/A
```

b) Visualizar puertos abiertos del equipo atacado

Solución:

```
ricardo@ricardo-VirtualBox:~$ nmap -sV -sC 192.168.60.43
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-26 10:17 CEST
Nmap scan report for 192.168.60.43
Host is up (0.032s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

c) Captura los paquetes de la red

Creamos un flujo de paquetes ICMP con la máquina 1 a la 3

```

ricardo@ricardo-VirtualBox: ~$ ping 192.168.60.43
PING 192.168.60.43 (192.168.60.43) 56(84) bytes of data.
64 bytes from 192.168.60.43: icmp_seq=1 ttl=128 time=132 ms
64 bytes from 192.168.60.43: icmp_seq=2 ttl=128 time=174 ms
64 bytes from 192.168.60.43: icmp_seq=3 ttl=128 time=82.1 ms
64 bytes from 192.168.60.43: icmp_seq=4 ttl=128 time=106 ms
64 bytes from 192.168.60.43: icmp_seq=5 ttl=128 time=319 ms
64 bytes from 192.168.60.43: icmp_seq=7 ttl=128 time=684 ms
64 bytes from 192.168.60.43: icmp_seq=9 ttl=128 time=291 ms
64 bytes from 192.168.60.43: icmp_seq=11 ttl=128 time=639 ms
64 bytes from 192.168.60.43: icmp_seq=12 ttl=128 time=472 ms
64 bytes from 192.168.60.43: icmp_seq=13 ttl=128 time=433 ms
64 bytes from 192.168.60.43: icmp_seq=15 ttl=128 time=683 ms
64 bytes from 192.168.60.43: icmp_seq=17 ttl=128 time=97.1 ms
64 bytes from 192.168.60.43: icmp_seq=19 ttl=128 time=542 ms
64 bytes from 192.168.60.43: icmp_seq=20 ttl=128 time=440 ms
64 bytes from 192.168.60.43: icmp_seq=21 ttl=128 time=578 ms
64 bytes from 192.168.60.43: icmp_seq=22 ttl=128 time=84.3 ms
64 bytes from 192.168.60.43: icmp_seq=23 ttl=128 time=139 ms
64 bytes from 192.168.60.43: icmp_seq=24 ttl=128 time=41.6 ms
64 bytes from 192.168.60.43: icmp_seq=26 ttl=128 time=48.7 ms
64 bytes from 192.168.60.43: icmp_seq=27 ttl=128 time=490 ms
64 bytes from 192.168.60.43: icmp_seq=28 ttl=128 time=111 ms
64 bytes from 192.168.60.43: icmp_seq=29 ttl=128 time=100 ms

```

Y desde la maquina 2 Con Whire Shark capturamos los paquetes ICMP

No.	Time	Source	Destination	Protocol	Length	Info
558	16.896348395	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
562	18.223991962	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
789	46.461822490	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
789	46.892850200	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
792	49.392252626	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
1227	76.543888889	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
1382	79.548632866	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
1615	187.323818834	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
1621	188.813437907	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
1530	119.538239850	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
2068	137.447932639	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
2128	140.488172292	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
2440	167.122597054	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
2444	168.639934821	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
2453	170.154229279	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
2741	199.988831682	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
2779	199.485275946	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)
2828	199.988889787	192.168.60.229	192.168.60.43	ICMP	122	Destination unreachable (Port unreachable)

Frame 558: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface any, id 0

- Linux cooked capture v2
- Internet Protocol Version 4, Src: 192.168.60.229, Dst: 192.168.60.43
- Internet Control Message Protocol
- NetBIOS Name Service

0000 00 04 00 01 00 06 08 09 27 72 71 bc 2d 6b 98 00rq-k.....
0020 45 c0 00 6a f2 b4 00 00 40 01 0c 06 c9 a8 3c e5 E.....<.....N
0040 c0 a8 3c 2b 03 03 f7 a9 80 00 00 00 45 00 00 4e <.....E.....
0060 e0 bc 00 00 88 11 5f 81 c0 a8 3c 2b c0 a8 3c e5<.....
0080 00 00 00 00 00 3c 1c 3f 01 0e 00 00 01 00 00?.....
00a0 00 00 00 00 29 43 40 41 41 41 41 41 41 41 41KA.AAAAAA
00c0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41AAAAA.AAAAAA
00e0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41AAAAA.AAAAAA
00f0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41AAAAA.AAAAAA

d) Cerrar y abrir puertos en Linux y Windows

Solución:

Windows

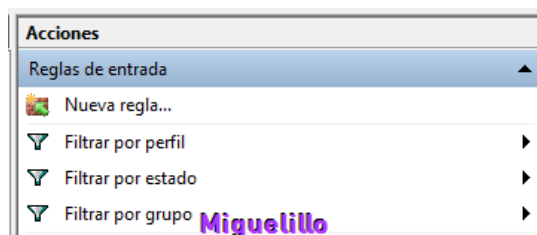
Para abrir y cerrar puertos en Windows

Vamos a **Panel de Control > Sistema y seguridad > Firewall de Windows Defender > Configuración Avanzada**

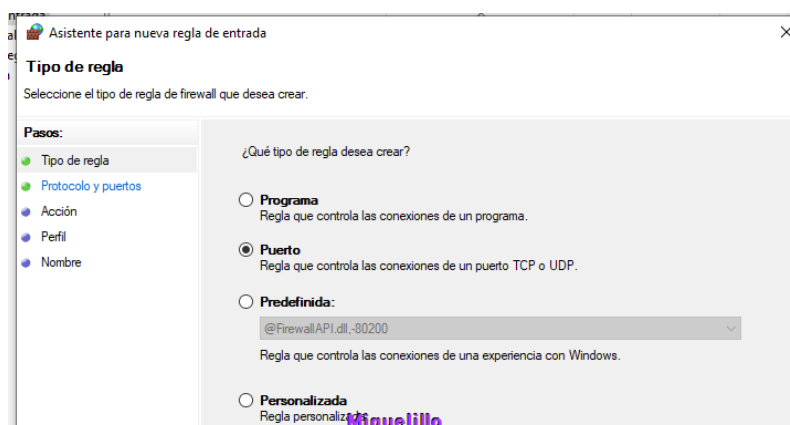
Una vez aquí podemos elegir entre reglas de entrada o de salida, dependiendo de si queremos activar o desactivar el puerto con un servicio que intente entrar o uno que quiera salir.



Seleccionamos por ejemplo Reglas de entrada y Clicamos en **Nueva Regla...**



Seleccionamos **Puerto**



Especificamos si es TCP o UDP y el número de puerto que queremos abrir o cerrar

¿Se aplica esta regla a TCP o UDP?

☒ TCP

☐ UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

☐ Todos los puertos locales

☒ Puertos locales específicos:

Ejemplo: 80, 443, 5000-5010

Miguelillo

Decimos si queremos permitir o bloquear el puerto

Asistente para nueva regla de entrada

Acción

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☒ Permitir la conexión

Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ Permitir la conexión si es segura

Esto incluye solamente las conexiones autenticadas mediante IPsec. Estas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

☐ Bloquear la conexión

Miguelillo

Declaramos en que perfil de red queremos

Asistente para nueva regla de entrada

Perfil

Especifique los perfiles en los que se va a aplicar esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Cuándo se aplica esta regla?

☒ Dominio

Se aplica cuando un equipo está conectado a su dominio corporativo.

☒ Privado

Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.

☒ Público

Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

Miguelillo

LINUX

Para abrir un puerto utilizaremos este comando dónde con **-A** indicamos que crearemos una **regla nueva** y pondremos **OUTPUT** o **INPUT** según si queremos que sea la regla de **entrada** o de **salida**, **-p** para especificar **tcp** o **udp**, con **--dport** especificamos el puerto en este caso el **80** y con **-j** especificamos si queremos **admitir** el tráfico con **ACCEPT**, **bloquearlo** sin dar mensaje de error con **DROP** o **bloquearlo** dando un **mensaje de error** con **REJECT**.

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Si queremos **desactivar** el **puerto** simplemente tendremos que **borra** la **regla** configurada ya que si la borras por **defecto** los puertos están **desactivados**. La opción para borrar la regla es **-D**

```
iptables -D INPUT -p tcp --dport 80 -j ACCEPT
```



The screenshot shows a terminal window titled "Ubuntu [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu bar, there are tabs for "Actividades" and "Terminal". The terminal window shows the following commands and output:

```
usuario@usuario-miguel-SRI: ~  
usuario@usuario-miguel-SRI:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
[sudo] contraseña para usuario:  
usuario@usuario-miguel-SRI:~$ sudo iptables -D INPUT -p tcp --dport 80 -j ACCEPT  
[sudo] contraseña para usuario:  
usuario@usuario-miguel-SRI:~$ Miguelillo
```

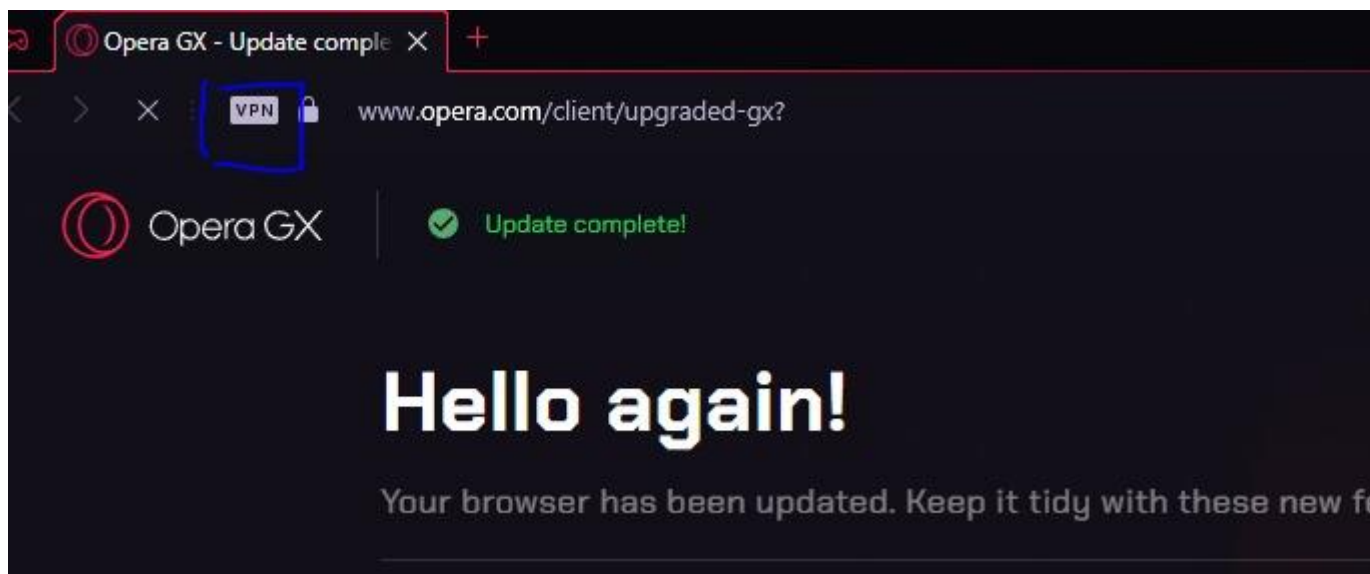

e) Para detectar sniffers

Solución:

Para detectar sniffers en la red no he encontrado ninguna herramienta específica, pero a nivel interno si que existen herramientas que los detectan como medida de protección como puede ser un Antivirus. He encontrado programas con los cual puedes evitar los sniffers como son las VPN estas se encargan de cifrar tus mensajes y que no sean visibles en texto claro, por lo cual si un paquete cae en manos de un sniffer no pueda leerlo.

Wireless Network Watcher									
File Edit View Options Help									
IP Address	Device Name	MAC Address	Network Adapter Company	Device Information	User Text	First Detected On	Last Detected On	Detection Count	Active
192.168.60.254		48-A9-8A-28-C0-B1	Routerboard.com	Your Router		26/09/2023 13:16:45	26/09/2023 14:24:39	3	Yes
192.168.60.253		00-31-92-D1-7E-B0	TP-Link Corporation Limited			26/09/2023 13:17:40	26/09/2023 14:25:14	2	Yes
192.168.60.250	DESKTOP-3I954N4	50-C2-E8-8E-2D-68	CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.		DESKTOP-3I954N4	26/09/2023 13:15:54	26/09/2023 14:25:14	3	Yes
192.168.60.235		BC-6A-D1-CB-43-E0	Xiaomi Communications Co Ltd			26/09/2023 13:35:58	26/09/2023 14:25:12	2	Yes
192.168.60.229	DESKTOP-KRURPG4	38-D5-7A-C2-61-4D	CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.		DESKTOP-KRURPG4	26/09/2023 13:17:09	26/09/2023 14:25:11	2	Yes
192.168.60.220	TONIPRINCIPAL	F8-0D-AC-0A-62-A4	HP Inc.		TONIPRINCIPAL	26/09/2023 13:28:46	26/09/2023 14:25:10	2	Yes
192.168.60.218		FE-B3-43-DA-2D-18				26/09/2023 13:19:29	26/09/2023 14:25:12	2	Yes
192.168.60.216	DESKTOP-RS9KCAM	50-EB-F6-4E-DA-39	ASUSTek COMPUTER INC.		DESKTOP-RS9KCAM	26/09/2023 13:17:08	26/09/2023 14:25:09	2	Yes
192.168.60.212	ASUS_JAVIER	14-13-33-6A-7D-D1	AzureWave Technology Inc.		ASUS_JAVIER	26/09/2023 13:53:54	26/09/2023 14:25:09	2	Yes
192.168.60.120	W10-01	34-E1-2D-16-40-81	Intel Corporate		W10-01	26/09/2023 13:26:02	26/09/2023 14:24:58	4	Yes
192.168.60.96	DESKTOP-11PUH05	04-92-26-15-B6-86	ASUSTek COMPUTER INC.		DESKTOP-11PUH05	26/09/2023 13:17:01	26/09/2023 14:24:55	3	Yes
192.168.60.81		04-0E-3C-52-79-6D	HP Inc.		DESKTOP-4SIHPD2	26/09/2023 13:18:18	26/09/2023 14:20:16	3	No
192.168.60.43	DESKTOP-7PEK6DG	08-00-27-E9-46-37	PCS Systemtechnik GmbH	Your Computer	DESKTOP-7PEK6DG	26/09/2023 13:15:41	26/09/2023 14:24:49	4	Yes
192.168.60.31	DESKTOP-8D4SD8I	34-6F-24-10-FD-2F	AzureWave Technology Inc.		DESKTOP-8D4SD8I	26/09/2023 13:16:59	26/09/2023 14:24:48	3	Yes
192.168.60.20		54-04-A6-F2-A3-DC	ASUSTek COMPUTER INC.			26/09/2023 13:16:54	26/09/2023 14:24:46	5	Yes
192.168.60.72	TONIPRINCIPAL	D8-C0-A6-70-83-95	AzureWave Technology Inc.		toniPRINCIPAL	26/09/2023 13:26:56	26/09/2023 14:05:57	2	No
192.168.60.209	DESKTOP-RS9KCAM	14-13-33-04-7D-B1	AzureWave Technology Inc.		DESKTOP-RS9KCAM	26/09/2023 14:06:03	26/09/2023 14:06:04	1	No

Miguelillo



Win10_SRI [Corriendo] - Oracle VM VirtualBox									
Archivo Máquina Ver Entradas Dispositivos Ayuda									
Ethereal									
Archivo Edición Visualización Captura Analizar Estadísticas Herramientas Ayuda									
No.	Time	Source	Destination	Protocol	Length	Info			
24330	955.670159	192.168.60.235	228.0.0.251	HTTP	162	Standard query 0x0000 a0v ("m"/"HOCU X3 Pro";"as":["8193",8194]";"ip":["228"]";_id=connect_udp_local;"Q" question SRV 0 0 50000 android.local			
12279	254.854506	192.168.60.235	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
11225	256.997496	192.168.60.235	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
6411	131.098554	192.168.60.235	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
6219	136.136127	192.168.60.235	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
4158	146.859674	192.168.60.235	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
2799	46.913152	192.168.60.235	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
7254	46.943721	192.168.60.235	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
2689	43.696679	192.168.60.235	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
40586	644.790221	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
26472	543.179736	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
26445	941.084572	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
15831	618.507280	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
25782	689.457534	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
25693	687.354789	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
24659	565.860838	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
24571	566.275749	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
24549	585.865996	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
22786	531.985678	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
22737	538.188380	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
12609	513.889094	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
22264	499.886664	192.168.60.229	192.168.60.43	TCP	60	Destination unreachable (Port unreachable)			
Frame 20535: 128 bytes on wire (968 bits) captured (968 bits) on interface "Device\NPF_{182AB845-2044-4784-9E13-F273718249}							0000 00 00 27 e9 46 37 38 05 7e c2 61 6d 00 00 45 c8E		
Ethernet II, Src: CloudNet_c201614d (38:0d:7a:c2:01:4d), Dst: PcsCompu_e946137 (00:00:27:e9:46:137)							0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
Internet Protocol Version 4, Src: 192.168.60.229, Dst: 192.168.60.43							0020 3c 20 03 03 77 00 00 00 00 45 00 00 46 c1 67E..g		
Internet Control Message Protocol							0030 00 00 00 11 5e 05 c8 a8 3c 20 c8 a8 3c 05 00 00<<-		
NetBios Name Service							0040 00 00 00 3a 10 c8 05 00 00 00 00 00 00 00AAAA		
							0050 00 00 20 43 40 41 41 41 41 41 41 41 41 41 41AAAA		
							0060 41 41 41 41 41 41 41 41 41 41 41 41 41 41AAAA		
							0070 41 41 41 00 00 21 00 01AAA		

Miguelillo