UT01: Adopción de pautas de seguridad informática – Amenazas 3 – Ataques de Reconocimiento

Nombre: Francisco Jesús García – Uceda Díaz – Albo y Alex Valdepeñas Curso: 2º ASIR.

Índice

Reconocimiento1
Introducción2
Desde el ordenador atacante (PC1-Windows/Linux): (Va todo en conjunto)2
a) Barrido de pings y detectar el sistema operativo de los equipos activos en la red (comando o herramientas: Superscan, IP Scanner, etc)
b) Visualizar o escanear los puertos que tiene abiertos el ordenador amenazado (PC3) 2
c) Captura los paquetes de la red desde "Man in the Midle" situado en PC2 (Windows/Linux).
Desde el ordenador amenazado (PC3 –Windows/Linux):11
a) Cerrar o abrir puertos (Windows y Linux)11
b) Realiza un informe sobre software anti-sniffers Y SI LO CONSIDERAS NECESARIO UTILIZA EL MISMO para detectar desde PC3 sniffers situados en la red11
Informe sobre Anti-Sniffer16
Conclusión

Introducción

En está práctica aprenderemos a realizar un ataque de reconocimiento a un equipo. Está práctica la hemos realizado con el compañero Alex Valdepeñas el cuál él es la víctima y yo el que realiza el ataque de reconocimiento. En la práctica aprenderemos también ha realizar un Man In The Middel e intentaremos interceptar a este.

Desde el ordenador atacante (PC1-Windows/Linux): (Va todo en conjunto).

a) Barrido de pings y detectar el sistema operativo de los equipos activos en la red (comando o herramientas: Superscan, IP Scanner, etc).

b) Visualizar o escanear los puertos que tiene abiertos el ordenador amenazado (PC3).

c) Captura los paquetes de la red desde "Man in the Midle" situado en PC2 (Windows/Linux).

El barrido de ping es utilizado para contabilizar las máquinas disponibles en una red, o monitorizar servidores. Es más fiable que hacer ping a la dirección de broadcast, ya que algunos equipos no responden a ese tipo de consultas.

Primero lo haremos con NMAP el escaneo, usaremos un escaneo rápido sobre la red 192.168.70/24 para encontrar el equipo que buscamos.

👁 Zenmap			
Escaneo Herramientas P	erfil Ayuda (<u>H</u>)		
Objetivo: 192.168.70.0/24	▼ Perfil: Quick scan ▼	Escaneo	Cancelar
Comando: nmap -T4 -F 19	2.168.70.0/24		
Servidores Servicios	Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos		
OS 4 Servidor 🔺	nmap -T4 -F 192.168.70.0/24	•	Detalles
	Starting Nmap 7.80 (https://nmap.org) at 2019-10-09 12:27 Hora de verano romance		
Filtrar servidores			

Como vemos, nos ha hecho un análisis con todas las máquinas que hay en la red, nosotros nos fijaremos en la .70.82 que es la máquina del compañero y de la cual podemos actuar.



Podemos también hacer un << Ping scan>> en toda la red.

🗢 Zenmap	
Escanen Herramientas Perfil Ayuda (H)	
Objetivo: 192.168.70.0/24 Perfil: Ping scan Compander: pman.scn 192.168.70.0/24 Perfil: Ping scan	▼ Escaneo Cancelar
Comando, Imap - 51 132.106.70.0/24	
Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos	
OS 4 Servidor A nmap -sn 192.168.70.0/24	▼ Detalles
192.168.70.7 Host is up (0. 031; 1 starsy)	A
192168 7011 Mac Address: 80:CE:CB:14:5C:14 (Hewlett Packard)	
Nmap scan report for 192.168.70.61	
192.168./0.18 Host is up (0.14s latency).	
192.168.70.20	
192.168.70.36 Host is up (0.078s latency).	
MAC Address: 18:CF:5E:21:0C:DD (Liteon Technology)	
Handpace Total Host is up (0.165 latency).	
MAC Address: B4:6B:FC:6E:70:CB (Intel Corporate)	
192.168.70.66 Nmap scan report for 192.168.70.81	
192.168.70.71 MAC Address: 7C:2A:31:5F:EB:FA (Intel Corporate)	
■ 192.168.70.81 Nmap scan report for 192.168.70.82	Ξ
19216870.82 MAL Address (2:24:31:52:E8:FA (Intel Corporate)	
Nmap scan report for 192.168.70.86	
Host is up (0.23s latency).	
192.168.70.91 Nmar scan report for 192.168.70.91	
192.168.70.108 Host is up (0.093s latency).	
192.168.70.114 Nac scan report for 192.168.70.108	
192168.70.115 Host is up (0.22s latency).	
MAC Address: 34:41:50:01:96:45 (Intel Corporate)	
Hold Figure The start of the st	
MAC Address: 34:41:5D:01:96:45 (Intel Corporate)	
■ 192.168.70.130 Nmap scan report for 192.168.70.115	
192.168.70.132 MAC Address: 34:E1:20:F6:64:C6 (Intel Corporate)	
192.168.70.189 Nmap scan report for 192.168.70.126	
Mac Address: F8:28:19:10:E:D8:67 (Liteon Technology)	
Filtrar servidores	-

Podemos realizar un escaneo con la versión ligera de nmap también:

nmap -T4 -F 192.168.70.0/24



Lo siguiente que haremos es descargar *Advamnced IP Scanner* para realizar un escaneo a la red con este programa. Puedes descargarlo pulsando <u>aquí.</u>



Podemos elegir instalarlo o su versión portable.

🖳 Instalar - Advanced IP Scanner 2.5	
Bienvenido al asistente de instalación de Advanced IP Scanner 2. Indique si desea instalar Advanced IP Scanner 2.5 o simplemente ejecutar	; 10.
Seleccionar acción: Instalar El programa se instalará. Para ajustes avanzados, marque la casilla "Co avanzada".	onfiguración
Ejecutar Ejecutar versión portátil (no es necesaria instalación).	
Configuración avanzada	
Siguiente >	Cancelar

Aceptaremos los términos y condiciones.

🛃 Instalar - Advanced IP Scanner 2.5	
Acuerdo de Licencia Es importante que lea la siguiente información antes de continuar.	ସ
Por favor, lea el siguiente acuerdo de licencia. Debe aceptar las cláusulas de este acuerdo antes de continuar con la instalación.	
Advanced IP Scanner	
END USER LICENSE AGREEMENT	
NOTICE TO USER:	-
 Acepto el acuerdo No acepto el acuerdo 	
< Atrás 🔞 Instalar 🛛	Cancelar

Para hacer un escaneo de la red basta con poner la IP de la red y darle explorar.

🔁 Advanced IP Sc	anner						•
Archivo Vista	Configuración Ayuda						
Explorar							
192.168.70.0/24						Ejemplo: 192.168.0.1-100, 192.168.0.200 Buscar	Q
Lista de resultados	Favoritos						
Estado	Nombre	ÍP	Fabricante	Dirección MAC	Comentarios		*
	DESKTOP-E9ALKGD	192.168.70.7	ASUSTek COMPUTER INC.	54:04:A6:F2:A6:9B			
	DESKTOP-NJFQ6CA	192.168.70.11	ASUSTek COMPUTER INC.	C8:60:00:9E:77:22			
	192.168.70.18	192.168.70.18	Cisco Systems, Inc	30:F7:0D:A7:4F:35			
Þ 📮	PC00ASIR2	192.168.70.20	ASUSTek COMPUTER INC.	54:04:A6:F2:A3:DC			
	192.168.70.36	192.168.70.36	Intel Corporate	64:5D:86:93:91:6C			
	DESKTOP-PARBVGK	192.168.70.46	Hewlett Packard	80:CE:62:14:5C:14			
	192.168.70.51	192.168.70.51	PCS Systemtechnik GmbH	08:00:27:9A:F1:44			
i	192.168.70.58	192.168.70.58	Shenzhen TINNO Mobile Technology	BC:41:01:2D:52:E2			
i -	DESKTOP-3UTRUJK	192.168.70.61	Hon Hai Precision Ind. Co.,Ltd.	A8:A7:95:3F:A6:BF			
i	192.168.70.66	192.168.70.66	Liteon Technology Corporation	18:CF:5E:21:0C:DD			
i -	DESKTOP-PO5GVTE	192.168.70.71	Intel Corporate	B4:6B:FC:6E:70:CB			E
	MSI	192,168,70,81	Intel Corporate	7C-2A-31-5E-ER-EA			
	W7	192.168.70.82	Intel Corporate	7C:2A:31:5F:EB:FA			
	ANGEL-PC	192.168.70.86	Intel Corporate	30:E3:7A:63:96:C4			
	DESKTOP-P7HG5NA	192.168.70.91	CyberTAN Technology Inc.	60:14:B3:AE:F4:87			
	LAPTOP-EV4N1I2U	192.168.70.101	Liteon Technology Corporation	F8:A2:D6:BB:71:15			
	LAPTOP-2ME9567F	192.168.70.108	Intel Corporate	34:41:5D:01:96:45			
i	192.168.70.110	192.168.70.110	HUAWEI TECHNOLOGIES CO., LTD	4C:D1:A1:C8:A0:23			
i	192.168.70.111	192.168.70.111		74:59:09:4C:EB:C0			
i	192.168.70.114	192.168.70.114	Intel Corporate	34:41:5D:01:96:45			
i 🚊	LAPTOP-O46RVBFK	192.168.70.115	Intel Corporate	34:E1:2D:F6:6A:C6			
i 🚊	192.168.70.121	192.168.70.121	CyberTAN Technology Inc.	60:14:B3:AE:F4:87			
i 🚊	LAPTOP-BID3T588	192.168.70.122	Liteon Technology Corporation	C8:FF:28:29:40:DD			
i 🚊	192.168.70.125	192.168.70.125	Xiaomi Communications Co Ltd	04:B1:67:AD:A8:31			
i 🚊	LENOVO-FRAN	192.168.70.126	Liteon Technology Corporation	F8:28:19:CE:D8:67			
🚊	Fran-PC	192.168.70.128	PCS Systemtechnik GmbH	08:00:27:6E:E6:9B			
II 🚊 🗌	192.168.70.130	192.168.70.130	Liteon Technology Corporation	F8:A2:D6:BB:71:15			
	WIN-HCI6VNVCGGC	192.168.70.132	PCS Systemtechnik GmbH	08:00:27:2F:28:E8			-
35 activo 1 inactivo	220 desconocido						

Podemos activar en las opciones más opciones para que nos de más información.

🙋 A	dvanced IP Sca	anner									
Arch	ivo Vista	Configuración Ayuda									
	Conterer	Opciones	-								
	Explorat	Idioma 🕨	-								
192.	168.70.82								Ejempla: 192.168.0.1-10	0, 192.168.0.200 Buscar	٩,
List	de resultados	Favoritos									
	Estado	Nor	bre	Ŷ	Grupo NetBIOS	Fabricante	Dirección MAC	Usuario	Fecha	Comentarios	
		W7		192.168.70.82	WORKGROUP	PCS Systemtechnik GmbH	08:00:27:0B:C0:DB		2019-10-09 12:47:23 UTC+02:00		

	 2010
Funcionamiento Recursos Otras	2019

🛃 Advanced IP Scanner							
Archivo Vista Configuración Ayuda							
Explorar							
192.168.70.82						Ejemplo: 192.168.0.1-100,	192.168.0.200 Buscar
Lista de resultados Favoritos							
Estado Nombre	ÍP	Grupo NetBIOS	Fabricante	Dirección MAC	Usuario	Fecha	Comentarios
📮 W7	192.168.70.82	WORKGROUP	PCS Systemtechnik GmbH	08:00:27:0B:C0:DB		2019-10-09 12:47:23 UTC+02:00	

Lo siguiente que haremos es descargar *Advanced Port Scanner*, un programa de la misma compañía, con este realizaremos un escaneo de puertos. Lo podemos descargar desde <u>aquí</u>.



Lo podremos de igual forma instalar o ejecutar en la versión portable.

🗺 Instalar - Advanced Port Scanner 2.5	- • •
Bienvenido al asistente de instalación de Advanced Port Scanner Indique si desea instalar Advanced Port Scanner 2.5 o simplemente ejecut	2.5 tario.
Seleccionar acción:	
 Instalar El programa se instalará. Para ajustes avanzados, marque la casilla "Co avanzada". Ejecutar Ejecutar versión portátil (no es necesaria instalación). 	onfiguración
Configuración avanzada	
Siguiente >	Cancelar

Vemos como según los puertos que encuentra en tiempo real lo va indicando, buscaremos directamente por la IP del equipo.

C Advanced Port Scanner			
Archivo Vista Configuración Ayuda			
Detener			
192.168.70.82		Puertos TCP conocidos 1-65535	Buscar
Lista de resultados Favoritos			
Estado Nombre	IP Grupo NetBIOS Fabricante	Dirección MAC	
📮 W7	192.168.70.82 WORKGROUP PCS Systemtechnik GmbH	08:00:27:0B:C0:DB	
		W7	
		Estado: Siletama operativ PAC: Fabricante: RetBIOS: Usuario: Tipo: Fecha: Comentarios: Servicio técnico Port 13S (TCP)	X Activo X 192.163.7082 06:00:27:08:CD:08 PCS Systematchik GmbH WORKGROUPW/7 2019-10-09 13:14:03 UTC+02:00 Mas información
•		Þ	
54% 1 active. 0 inactive. 0 descenocide			

Con un escaneo rápido en ZENMAP también podremos ver los puertos abiertos del equipo que buscamos, vemos como tiene varios puertos abiertos, en este caso cerraremos el puerto NetBIOS (Podremos ver como se hace en la segunda parte sección A de este ejercicio).

🗢 Zenmap		_ 0 🗾
Esc <u>a</u> neo Herramien <u>t</u> as	Perfil Ayuda (H)	
Objetivo: 192.168.70.82	Perfit:	▼ Escaneo Cancela
Comando: nmap -T4 -F	92.168.70.82	
Servidores Servicios	Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos nmap -T4 -F 192.168.70.82	▼ ≣ Detalles
 192.168.70.81 192.168.70.82 	Starting Nmap 7.80 (https://nmap.org) at 2019-10-09 13:29 Hora de verano romance Nmap scan report for 192.168.70.82 Host is up (0.0408 latency).	
■ 192.168./0.126	PORT STATE SERVICE 135/trp open 139/trp open 139/trp open 139/trp open 139/trp open 139/trp open 135/trp open 155/trp open 155/trp open 15/trp open 15/trp open 15/trp open 15/trp open 16/trp 17/trp open 18/trp 18/trp 18/trp open 18/trp open 1	

Una vez cerrado podemos ver que ya no nos aparece.

👁 Zenmap		
Esc <u>a</u> neo Herramien <u>t</u> as <u>P</u> e	erfil Ayuda (H)	
Objetivo: 192.168.70.82	▼ Perfil:	Escaneo Cancelar
Comando: nmap -T4 -F 19	2.168.70.82	
Servidores Servicios OS 4 Servidor 192.168.70.81 192.168.70.82 192.168.70.126 192.168.70.126	Salida Nmap Puertos / Servidores Topologia Detalles del servidor Escaneos nmap -T4 -F192168.70.82	▼ ≣ Detalles

Si eliminamos la regla y reiniciamos el equipo de la victima podemos ver como se vuelve a abrir.

👁 Zenmap				
Esc <u>a</u> neo Herramien <u>t</u> as	<u>P</u> erfil Ayuda (<u>H</u>)			
Objetivo: 192.168.70.82	Perfit:	•	Escaneo	Cancela
Comando: nmap -p 1-10	23 192.168.70.82			
Servidores Servicios	Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos			
OS 4 Servidor 🔺	nmap -p 1-1023 192.168.70.82		-	Detalles
 192.168.70.81 192.168.70.82 192.168.70.126 	Starting Nmap 7.80 (https://nmap.org) at 2019-10-09 13:40 Hora de verano romance Nmap scan report for 192.168.70.82 Host is up (0.0145 latency). Not shown: 1020 closed ports PORT STATE SERVICE 135/tcp open msrpc 139/tcp open metbios-ssn 445/tcp open microsoft-ds MAC Address: 7C:2A:31:5F:EB:FA (Intel Corporate)			
	<u>Nmap done:</u> 1 IP address (1 host up) scanned in 38.49 seconds			

A partir de esta parte lo hemos realizado en una máquina con <u>Ubuntu 18</u> instalado, como vemos esta máquina no tiene ningún puerto abierto.



Con *nmap -p* [*rango puertos*] [IP] podremos buscar por rango de puertos.

Lo que hemos realizado y que veremos en la segunda parte sección a es como abrir puertos, vemos que en *State* aparece como *Closed*, esto ocurre porque en Ubuntu, todos los puertos se abren a menos que tenga un firewall o una aplicación que lo esté bloqueando. En circunstancias normales, la aplicación que se ejecuta en el puerto es para escuchar.

Un puerto generalmente se considera abierto cuando hay un programa ejecutándose y escuchando en el puerto.

• Zenmap		• 🗙
Esc <u>a</u> neo Herramien <u>t</u> as <u>P</u> erfil Ayuda (<u>H</u>)		
Objetivo: 192.168.70.130 Perfil: Quick scan	Escaneo	Cancelar
Comando: nmap - T4 - F 192.168.70.130		
Servidores Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos		
OS 4 Servidor 🔺 nmap -T4 - F 192.168.70.130	▼ ≣	Detalles
 I92.168.70.81 Starting Nmap 7.80 (https://nmap.org) at 2019-10-09 14:24 Hora de verano romance Nmap scan report for 192.168.70.130 Host is up (0.008 latency). I92.168.70.130 Not shown: 97 filtered ports PORT STATE SERVICE 80/tcp closed http 3306/tcp closed http-proxy MAC Address: 08:00:27:68:C3:C8 (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds 		

Como vemos hemos abierto el puerto http, MySQL y http-proxy.

Hemos cerrado el puerto MySQL y hemos abierto el https (443).

Zenmap	
Esc <u>a</u> neo Herramien <u>t</u> as <u>P</u>	erfil Ayuda (H)
Objetivo: 192.168.70.130	Perfil: Quick scan
Comando: nmap -T4 -F 19	22.168.70.130
Servidores Servicios	Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos
OS 4 Servidor 🔺	nmap - T4 - F 192.168.70.130
₩ 192.168.70.130	Starting Nmap 7.80 (https://nmap.org) at 2019-10-09 18:32 Hora de verano romance Nmap scan report for 192.168.70.130 Host is up (0.00066s latency). Not shown: 97 filtered ports PORT STATE SERVICE 80/tcp closed http 443/tcp closed http- 8080/tcp closed http-proxy MAC Address: 08:00:27:68:C3:C8 (Oracle VirtualBox virtual NIC)
	<pre>Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds</pre>

La siguiente fase será realizar un Man In The Middel en los equipos, podemos ver el escenario. Para realizar el MiNT utilizaremos Wireshark. Capturaremos la clave de usuario de una página http.

Ed 🗔 🍨 Expre
rface θ (c8:1f:be:6e
tn: 792
>
Î
Î
*

Time 204 20.145192 214 20.476259					🖾 🗔 *) Expression	. 4
214 20.476259	Source 192.168.100.3	Destination 185,28,20,195	Protocol Length Info HTTP 591 GET / HTTP/	1.1		
216 20 525011	185.28.20.195	192.168.100.3	HTTP 60 HTTP/1.1 20	0 OK (text/html))	
216 20.625944	192.168.100.3	185.28.20.195	HTTP 573 GET /theme/	wood/styles.php	HTTP/1.1	
220 20.682315	185.28.20.195	192.168.100.3	HTTP 430 HTTP/1.1 20	0 OK (text/html))	
224 20.683144	185.28.20.195	192.168.100.3	HTTP 60 HTTP/1.1 20	0 OK (text/css)		
235 23.306586	192.108.100.3	192.168.100.3	HTTP 60 HTTP/1.1 20	0 OK (text/html)	
257 30.368248	192.168.100.3	185.28.20.195	HTTP 846 POST /login	/index.php HTTP/	1.1 (application/x-www-form-urlencoded)	
1296 119.954455	195.28.20.105 192.168.100.3	192.168.199.3 185.28.20.195	HTTP 60 HTTP/1/1 20 HTTP 843 POST /login	/index.php HTTP/	1.1 (application/x-www-form-unlencoded)	
1309 120.025047	185.28.20.195	192.168.100.3	HTTP 60 HTTP/1.1 20	OK (te: Wire	shark - Packet 1296 - Wi-Fi - X	
				> Fr > Eti > In > Tr > Hy	ame 1206: 833 bytes on wire (6744 bits), 843 bytes captured (6744 bits) on interface 0 herent II, Scr: frazi@raccelaziza (faiz@raccelazia)a), Datt Hamweiit@racdfil@ (@8:1f:be:6e anmission Control Protocol, Scr: Part 132, 163, 100, J, Dat: 185, 28, 20, 195 anmission Control Protocol, Scr: Part 52784, Dst Port: 80, Seg: 1, Ack: 1, Len: 789 pertext Immedia prodoci.	
					Form item: "username" = "alex"	
Frame 1296: 843 byt Ethernet II. Src: f	tes on wire (6744 bi fa:28:ea:ce:3a:2a (f	its), 843 bytes captu fa:28:ea:ce:3a:2a), D	red (6744 bits) on interface (st: HuaweiTe 6e:df:10 (c8:1f:1	0 be:6e:df:1	Form item: "testcookies" = "1"	
Internet Protocol V	Version 4, Src: 192.	.168.100.3, Dst: 185.	28.20.195	L		
Transmission Contro	pl Protocol, Src Por	rt: 52784, Dst Port:	30, Seq: 1, Ack: 1, Len: 789	0000	c8 1f be 6e df 10 fa 28 ea ce 3a 2a 08 00 45 00 ····n···(··:*··E· ^	
HTML Form URL Encod	ded: application/x-w	www-form-urlencoded		0010	03 3d 08 e7 40 00 40 06 3c 49 c0 a8 64 03 b9 1c = @ @ @ <i -="" d<br="">14 c3 ce 30 00 50 18 d3 5a fc da ed 46 7c 50 18 0 P. i. FP.</i>	
> Form item: "user	name" = "alex"			0030	02 00 ab 70 00 00 50 4f 53 54 20 2f 6c 6f 67 69p. PO ST /logi	
> Form item: "test	cookies" = "1"			0848	6e 2f 69 6e 64 65 /8 2e /0 68 /0 20 48 54 54 50 n/index. php HTP 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 63 75 72 73 /1.1 Ho st: curs	
				0868	6f 73 2e 69 6e 66 6f 72 61 63 74 69 76 61 2e 6e os.infor activa.n	
				0070	6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 keep-ali ve Cont	
				0090	65 6e 74 2d 4c 65 6e 67 74 68 3a 20 34 36 0d 0a ent-Leng th: 46	
				0050	61 78 2d 61 67 65 3d 30 0d 0a 4f 72 69 67 69 6e ax-age=0Origin	
000 c8 1f be 6e df	10 fa 28 ea ce 3a	2a 08 00 45 00 ····	1(:*E-	00c0	3a 20 68 74 74 70 3a 2f 2f 63 75 72 73 6f 73 2e : http://cursos.	-
010 03 3d 08 e7 40 320 14 c3 ce 30 00	00 40 06 3c 49 c0 50 18 d3 6a fc da	a8 64 03 b9 1c -=- ed 46 7c 50 18	@@.@. <id .P jFIP.</id 			. 8
030 02 00 ab 70 00	00 50 4f 53 54 20	2f 6c 6f 67 69 ····	- PO ST /logi		Cerrar Ayuda	~
Cilo Edit View	Go. Conturo	Analuza Statisti	ss Talanhany Wireless	Tools Hole		
The Edit View	GO Capture	Analyze Statisti	ts relephony wheless			
[📕 🙋 🙂]	010 X G	५ ७ ⇒ ≌ ।	ે 🗿 📑 લ્ લ્	⊂, ₩		
Apply a display fil	ter <ctrl-></ctrl->				Expression	+
p. Time	Source		Destination	Protocol Le	enath Info	1
524 71,046	5515 PcsCo	mpu 5f:c7:c1	Broadcast	ARP	42 Who has 192,168,70,254? Tell 192,168,70,126	
525 71.040	5647 PcsCo	mpu_5f:c7:c1	Broadcast	ARP	42 Who has 216.58.201.174? Tell 192.168.70.126	
526 71.046	5768 2001:	cccc:10::10	ff02::1:ff00:1	TCMPv6	86 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1	
527 71.546	5458 PcsCo	ompu 5f:c7:c1	Broadcast	ARP	42 Who has 185.28.20.195? Tell 192.168.70.126	
528 71.546	5733 172.2	217.168.161	10.0.2.15	TCP	110 [TCP Retransmission] 443 → 49714 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6.	
529 72.046	5754 2001:	cccc:10::10	ff02::1:ff00:1	ICMPv6	86 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1	
530 72.094	1479 PcsCo	mpu_5f:c7:c1	Broadcast	ARP	42 Who has 216.58.201.174? Tell 192.168.70.126	
531 73.046	5231 PcsCo	ompu_5f:c7:c1	Broadcast	ARP	42 Who has 216.58.201.174? Tell 192.168.70.126	
532 73.077	7781 2001:	cccc:10::10	ff02::1:ff00:1	ICMPv6	86 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1	
	0540 0	ompu_5f:c7:c1	Broadcast	ARP		
533 73.609	954Z PCSCO				42 Who has 192.168.70.254? Tell 192.168.70.126	
533 73.609 534 74.046	5232 PcsCo	mpu_5f:c7:c1	Broadcast	ARP	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126	
533 73.609 534 74.046 535 74.046	5232 PcsCo 5279 2001:	ompu_5f:c7:c1 :cccc:10::10	Broadcast ff02::1:ff00:1	ARP ICMPv6	42 Who has 192.168.70.2547 Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 86 Neighbor Solicitation for 2001:ccc:10::11 from 08:00:27:5f:c7:c1	
533 73.609 534 74.046 535 74.046 536 74.546	5232 PCSC0 5232 PCSC0 5279 2001: 5676 PCSC0	ompu_5f:c7:c1 :cccc:10::10 ompu_5f:c7:c1	Broadcast ff02::1:ff00:1 Broadcast	ARP ICMPv6 ARP	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 86 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126	
533 73.609 534 74.046 535 74.046 536 74.546 537 74.546	542 PCSCO 5232 PCsCo 5279 2001: 5676 PCsCo 5679 8.248	ompu_5f:c7:c1 cccc:10::10 ompu_5f:c7:c1 3.239.254	Broadcast ff02::1:ff00:1 Broadcast 10.0.2.15	ARP ICMPv6 ARP TCP	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.291.174? Tell 192.168.70.126 86 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126 60 [TCP Retransmission] 80 → 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L.	
533 73.609 534 74.046 535 74.046 536 74.546 537 74.546 538 75.046	542 PCSC0 5232 PcsC0 5279 2001: 5676 PcsC0 5679 8.248 5351 2001:	<pre>pmpu_5f:c7:c1 ccccc:10::10 pmpu_5f:c7:c1 3.239.254 ccccc:10::10</pre>	Broadcast ff02::1:ff00:1 Broadcast 10.0.2.15 ff02::1:ff00:1	ARP ICMPv6 ARP TCP ICMPv6	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 86 Neighbor Solicitation for 2001:ccc:10::11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126 60 [TCP Retransmission] 80 ↔ 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 86 Neighbor Solicitation for 2001:cccc:10::11 from 08:00:27:5f:c7:c1	1
533 73.609 534 74.040 535 74.040 536 74.540 537 74.540 538 75.040 539 75.040	542 PCSC0 5232 PcsCo 5279 2001: 5676 PcsCo 5677 8.248 5351 2001: 5507 52.14	<pre>pmpu_5f:c7:c1 ccccc:10::10 pmpu_5f:c7:c1 3.239.254 ccccc:10::10 42.84.61</pre>	Broadcast ff02::1:ff00:1 Broadcast 10.0.2.15 ff02::1:ff00:1 10.0.2.15	ARP ICMPv6 ARP TCP ICMPv6 TCP	42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 86 Weighbor Solicitation for 2001:ccc:10::1 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 60 [TCP Retransmission] 80 → 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 86 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=65	
533 73.609 534 74.046 535 74.046 536 74.546 537 74.546 538 75.046 539 75.046 540 75.343	542 PCSC0 5232 PcsCo 5279 2001: 5676 PcsCo 5677 8.248 5351 2001: 5507 52.14 3306 PcsCo	<pre>pmpu_5f:c7:c1 ccccc:10::10 pmpu_5f:c7:c1 3.239.254 ccccc:10::10 42.84.61 pmpu_5f:c7:c1</pre>	Broadcast ff02::1:ff00:1 Broadcast 10.0.2.15 ff02::1:ff00:1 10.0.2.15 Broadcast	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 86 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126 60 [TCP Retransmission] 80 → 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 86 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6. 42 Who has 216.58.201.174? Tell 192.168.70.126	
533 73.609 534 74.046 535 74.046 536 74.546 537 74.546 538 75.046 539 75.046 539 75.046 540 75.343 541 75.546	542 Pesco 5232 Pesco 5279 2001: 5676 Pesco 5677 8.248 5351 2001: 5507 52.14 3306 Pesco 5222 Pesco	<pre>pmpu_5f:c7:c1 ccccc:10::10 pmpu_5f:c7:c1 3.239.254 ccccc:10::10 42.84.61 pmpu_5f:c7:c1 pmpu_5f:c7:c1</pre>	Broadcast ff02::1:ff00:1 Broadcast 10.0.2.15 ff02::1:ff00:1 10.0.2.15 Broadcast Broadcast	ARP ICMPv6 ARP ICP ICMPv6 TCP ARP ARP	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 43 Michael Schultz 192.168.70.126 44 Who has 192.168.70.254? Tell 192.168.70.126 45 (TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L 46 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 + 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=65 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126	
533 73.609 534 74.044 535 74.044 536 74.546 537 74.546 538 75.046 539 75.046 540 75.343 541 75.546 542 75.578	542 PCSCo 5232 PCSCo 5279 2001: 5676 PCSCo 5677 8.248 5351 2001: 5507 52.14 3306 PCSCo 2222 PCSCo 8164 PCSCo	<pre>>mpu_5f:c7:c1 >cccc:10::10 >mpu_5f:c7:c1 \$.239.254 *ccccc:10::10 *2.84.61 >mpu_5f:c7:c1 >mpu_5f:c7:c1 >mpu_5f:c7:c1 >mpu_5f:c7:c1</pre>	Broadcast ff02::1:ff00:1 Broadcast 10.0.2.15 ff02::1:ff00:1 10.0.2.15 Broadcast Broadcast Broadcast	ARP ICMPv6 ARP ICP ICMPv6 TCP ARP ARP ARP	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 48 Weighbor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126 46 Weighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49791 [FIN, PSH, ACK] Seq=1 Ack=1 Win=65 42 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 195.28.20.195? Tell 192.168.70.126	
533 73.605 534 74.044 535 74.044 536 74.546 537 74.546 538 75.046 539 75.046 540 75.343 541 75.546 542 75.578 543 76.046	542 PCSCo 5232 PCSCo 5279 2001: 5676 PCSCo 5677 8.248 5351 2001: 5507 52.14 3306 PCSCo 5222 PCSCo 5164 PCSCo 5484 PCSCo	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	Broadcast ff02:11:ff00:1 Broadcast 10:0.2.15 ff02:11:ff00:1 10:0.2.15 Broadcast Broadcast Broadcast Broadcast	ARP ICMPv6 ARP ICMPv6 TCP ARP ARP ARP ARP	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 46 Weighbor Solicitation for 2001:cccc:10::11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126 60 [TCP Retransmission] 80 → 49695 [FIN, ACK] Seq=1 Ack=1 Win=5535 L. 86 Neighbor Solicitation for 2001:ccccc:10::1 from 08:00:27:5f:c7:c1 122 [TCP Retransmission] 433 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6. 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 195.168.70.254? Tell 192.168.70.126 42 Who has 185.28.20.195? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126	
533 73.605 534 74.044 535 74.044 536 74.546 537 74.546 539 75.044 539 75.044 540 75.343 541 75.546 542 75.578 543 76.046	542 PCSC0 5232 PcsC0 5279 2001: 5676 PcsC0 5677 8.248 5351 2001: 5507 52.14 3306 PcsC0 5222 PcsC0 8164 PcsC0 484 PcsC0 1 butce pcsC1	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	Broadcast ff02:11:ff00:1 Broadcast 10.0.2.15 ff02:11:ff00:1 10.0.2.15 Broadcast Broadcast Broadcast Broadcast Broadcast	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 60 [TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L 60 [TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L 60 Reighbor Solicitation for 2001:cccc:10::1 from 08:00:27:57:c7:c1 132 [TCP Retransmission] 43 + 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=65 42 Who has 192.165.70.254? Tell 192.168.70.126 42 Who has 192.165.70.254? Tell 192.168.70.126 42 Who has 185.28.20.195? Tell 192.168.70.126 42 Who has 185.28.20.174? Tell 192.168.70.126 42 Who has 185.28.20.174? Tell 192.168.70.126 42 Who has 185.82.00.174? Tell 192.168.70.126 43 Who has 185.82.00.174? Tell 192.168.70.126 44 Who has 185.82.00.174? Tell 192.168.70.126 45 Who has 185.82.00.174? Tell 192.168.70.126 46 Who has 185.82.00.174? Tell 192.168.70.126 47 Who has 185.82.00.174? Tell 192.168.70.126 48 Who has 185.82.00.174? Tell 192.168.70.126 47 Who has 185.82.00.174? Tell 192.168.70.126 48 Who has 185.82.00.174? Tell 192.168.70.126 48 Who has 185.82.00.174? Tell 192.168.70.126 49 Who has 185.70.201? Tell 192.168.70.126 40 Who has 185.70.201?	
533 73.600 534 74.044 535 74.044 536 74.546 537 74.546 539 75.046 539 75.046 549 75.343 541 75.546 542 75.576 542 75.376.046 Frame 27: 85 Fhemet 27:	2522 PCsCo 25279 2001: 5676 PcsCo 5676 PcsCo 5679 8.244 5551 2001: 5507 52.14 3306 PcsCo 5522 PcsCo 3164 PcsCo 5484 PcsCo 5484 PcsCo	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	Broadcast ff02::1:ff00:1 Broadcast 10.0:2.15 ff02::1:ff00:1 10.0:2.15 Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast	ARP ICMPv6 ARP ICMPv6 ICMPv6 TCP ARP ARP ARP (6808 bits)	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 58 Neighbor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126 50 [TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 50 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6. 42 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 195.28.20.195? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 43 Who has 216.58.201.174? Tell 192.168.70.126 44 Who has 216.58.201.174? Tell 192.168.70.126 45 Who has 216.58.201.174? Tell 192.	
533 73.600 534 74.044 535 74.044 536 74.044 538 75.046 538 75.046 538 75.046 540 75.343 541 75.576 543 76.046 Frame 27: 85 Ethernet II, Internet Por	222 PCsCo 2232 PCsCo 25279 2001: 3676 PCsCo 3679 8.248 3351 2001: 5507 52.14 3306 PCsCo 3522 PCsCo 3164 PCsCo 3484 PCsCo 3484 PCsCo 3484 PCsCo 3484 PCsCo	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	Broadcast ff02:1:ff00:1 Broadcast 10:0.2.15 ff02:1:ff00:1 10:0.2.15 Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast 00:27:5f:c7:c1), Dst	ARP ICMPv6 ARP TCP ICMPv6 ICMPv6 ARP ARP ARP ARP ARP (6808 bits) : RealtekU_1 195	42 Who has 192.168.70.254 [°] Tell 192.168.70.126 42 Who has 216.58.201.174 [°] Tell 192.168.70.126 86 Weighbor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 [°] Tell 192.168.70.126 60 [TCP Retransmission] 80 → 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 86 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 43 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=65 42 Who has 216.58.201.174 [°] Tell 192.168.70.126 42 Who has 192.168.70.254 [°] Tell 192.168.70.126 42 Who has 192.168.70.254 [°] Tell 192.168.70.126 42 Who has 195.28.201.95 [°] Tell 192.168.70.126 42 Who has 216.58.201.174 [°] Tell 192.168.70.126 42 Sequence 100 [Sequence 100] [Seq	
533 73.600 534 74.044 535 74.044 536 74.546 537 74.546 539 75.046 539 75.046 540 75.343 541 75.546 542 75.576 543 76.046 Frame 27: 85 Ethernet II, Internet Pro	2522 PCsCo 25279 2001: 2676 PcsCo 2679 2001: 2678 PcsCo 2527 2001: 2507 52:14 25507 52:14 25507 52:14 25522 PcsCo 25484 PcsCo	<pre>mpu_5f:c7:c1 cccc:10::10 mpu_5f:c7:c1 i.239.254 ccccc:10::10 i2.384.61 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 ec (6808 bits), u_5f:c7:c1(08: 4, Src:10.0.2 </pre>	Broadcast ff02:11:ff00:1 Broadcast 10:0.2.15 ff02:11:ff00:1 Broadcast	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP (6808 bits) : RealtekU_1 195 Sec: 1 4	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 43 Who has 216.58.201.174? Tell 192.168.70.126 46 Weighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126 46 Neighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 122 [TCP Retransmission] 43 → 49674 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 42 Who has 126.58.201.174? Tell 192.168.70.126 42 Who has 125.168.70.254? Tell 192.168.70.126 42 Who has 125.28.20.054? Tell 192.168.70.126 42 Who has 125.28.20.054? Tell 192.168.70.126 42 Who has 125.28.201.174? Tell 192.168.70.126 42 Who has 125.28.201.174? Tell 192.168.70.126 42 Who has 125.28.201.174? Tell 192.168.70.126 42 Who has 125.58.201.174? Tell 192.168.70.126 42 Who has 125.58.201.174? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 50 minterface 0 51 Minterface 0 51 Minterface 0 51 Minterface 0 52 Minterface 0 52 Minterface 0 53 Minterface 0 54 Minterface 0 54 Minterface 0 55 Minterface 0 56 Minterface 0 57 Minterface 0 57 Minterface 0 57 Minterface 0 58 Minterface 0 5	
533 73.600 534 74.044 535 74.044 536 74.944 537 74.544 538 75.046 539 75.046 539 75.046 540 75.343 541 75.546 542 75.576 543 76.046 Frame 27: 85 Ethernet II, Internet II, Internet Pro	2522 PCsCo 25279 2001: 5676 PcsCo 5679 8.248 5351 2001: 5507 52.14 3306 PcsCo 3306 PcsCo 3104 PcsCo 5484 PcsCo 5484 PcsCo 5484 PcsCo 5484 PcsCo 5648 PcsCo 57c: PcsComp tocol Version (Control Prot	<pre>mpu_sf:c7:c1 cccc:10:10 mpu_sf:c7:c1 i239,254 ccccc:10:10 i2.84.61 i2.84.61 impu_sf:c7:c1 impu_</pre>	Broadcast ff02:11:ff00:1 Broadcast 10.0.2.15 ff02:11:ff00:1 10.0.2.15 Broadcast Broadcast Broadcast Broadcast 851 bytes captured 00:27:5f:c7:c1), Dst 1.15, Dst: 185.28.20. 49841, Dst Port: 80	ARP ICMPv6 ARP ICMPv6 TCP ICMPv6 TCP ARP ARP ARP ARP (6808 bits) : RealtekU_1 195 ; Seq: 1, Ac	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 43 Who has 216.58.201.174? Tell 192.168.70.126 56 Neighbor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254? Tell 192.168.70.126 56 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=65 42 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 192.168.82.201.95? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 43 Who has 216.58.201.174? Tell 192.168.70.126 45 Who has 216.58.201.174? Tell 192.168.70.126 46 Who has 216.58.201.174? Tell 192.168.70.126 47 Who has 216.58.201.174? Tell 192.168.70.126 48 Who has 216.58.201.174? Tell 192.168.70.126 49 Who has 216.58.201.174? Tell 192.168.70.126 40 Who has 216.58.201.174? Tell 192.168.70.126 40 Who has 216.58.201.174? Tell 192.168.70.126 41 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 43 Who has 216.58.201.174? Tell 192.168.70.126 44 Who has 216.58.201.174? Tell 192.168.70.126 45 Who has 216.58.201.174? Tell 192.168.70.126 46 Who has 216.58.201.174? Tell 192.168.70.126 47 Who h	
533 73.600 534 74.040 535 74.044 536 74.540 538 75.040 539 75.040 539 75.040 540 75.343 541 75.576 543 76.040 Frame 27: 85 Ethernet II, Internet Pro Transmission	232 PCsCo 232 PCsCo 25279 2001: 5676 PcsCo 5679 8.248 3351 2001: 5507 52.14 3306 PcsCo 3516 PcsCo 3164 PcsCo 3	<pre>mpu_5f:c7:c1 cccc:10:10 mpu_5f:c7:c1 s.239.254 cccc:10:10 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 e (6808 bits), u_5f:c7:c1 (08: 4, Src:10.0.2 s.col, Src Port: 00 27 5f c7 c1</pre>	Broadcast ff02:1:ff00:1 Broadcast 10:0.2.15 ff02:1:ff00:1 10:0.2.15 Broadcast Boold Sold Sold Sold Sold Sold Sold Sold	ARP ICMPv6 ARP ICP ICMPv6 TCP ARP ARP ARP ARP ARP (6808 bits) : RealtekU_1 195 , Seq: 1, Ac	42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 68 Heighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 68 Heighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 43 → 49791 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6535 L 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.201.95 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 192.168.70.259 ³ Tell 192.168.70.126 42 Who has 192.168.70 ⁴ Tell 192.168.70.126 42 Who has 192.168.70 ⁴ Tell 192.168	
533 73.600 534 74.044 535 74.044 536 74.544 538 75.044 538 75.044 538 75.044 540 75.343 541 75.576 543 76.046 Frame 27: 85 Ethernet II, Internet Pro Transmission 000 52 54 00 010 03 45 56 010 04 45 27 010 14 45 17 010 14 14 14 14 14 14 14 14 14 14 14 14 14	2322 PCsCo 2327 PCsCo 2327 2001: 5676 PCsCo 5679 8.248 5557 52.14 2306 PCsCo 5222 PCsCo 3164 PCsCo 5222 PCsCo 11 bytes on wi Src: PCsComp tocol Version (2) 250 20 80 (35 40 00 80 (1) 25 60 00 10 (1) 25 60 00 00 (1) 25 60 00 00 (1) 25 60 00	<pre>mpu_5f:c7:c1 cccc:10::10 mpu_5f:c7:c1 i.239.254 cccc:10::10 i2.84.61 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 re (6808 bits), u_5f:c7:c1 (08: re (1</pre>	Broadcast ff02:11:ff00:1 Broadcast 10:0.2.15 ff02:11:ff00:1 10:0.2.15 Broadcast Broadcast Broadcast Broadcast 851 bytes captured 00:27:5f:c7:c1), Dst 1.15, Dst: 185.28.20. 49841, Dst Port: 80 08 00 45 00 RT-5 02 0f b9 1c · E^+@ 64 02 50 ° S	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP Seq: 1, Ad Seq: 1, Ad	42 Who has 192.168.70.254 [°] Tell 192.168.70.126 42 Who has 192.168.70.254 [°] Tell 192.168.70.126 42 Who has 216.58.201.174 [°] Tell 192.168.70.126 68 Heighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 [°] Tell 192.168.70.126 68 ICTCP Retransmission] 80 → 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 86 Neighbor Solicitation for 2001:ccccc:10::1 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 43 → 49674 [FIN, PSH, ACK] Seq=1 Ack=1 Win=65 42 Who has 192.168.70.254 [°] Tell 192.168.70.126 42 Who has 195.26.80.195 [°] Tell 192.168.70.126 42 Who has 185.28.20.195 [°] Tell 192.168.70.126 42 Who has 185.28.201.95 [°] Tell 192.168.70.126 42 Who has 195.28.201.95 [°] Tell 192.168.70.126 43 Who has 195.28.201.95 [°] Tell 192.168.70.126 44 Who has 195.28.201.95 [°] Tell 192.168.70.126 45 Who has 192.168.70.25 [°] Tell 192.168.70.126 46 Who has 192.168.70 [°] Tell 192.168.70.126 47 Who has 192.168.70 [°] Tell 192.168.70 [°]	
533 73.600 534 74.040 535 74.041 536 74.541 537 74.541 538 75.046 539 75.046 539 75.046 540 75.332 541 75.546 542 75.576 543 76.046 Frame 27: 85 Ethernet II, Internet Pro Transmission 000 82 54 00 100 03 45 56 1000 16 65 14 c3 c2 16 66 14 c3 c2 16 66 16 66 16 76 16 76 17 76 17 76 18 76 1	2532 PCSC0 2522 PCSC0 5676 PCSC0 5677 8.248 56351 2001: 5567 52.14 5567 52.14 5567 52.14 5567 52.24 5567 52.24 5567 52.24 5678 PCSC0 5222 PCSC0 5232 PCSC0 5484 PCSC0 57c: PCSC0mp 57c: PCSC0mp 57c: PCSC0mp 5579 80.80 60.80 80 60.80 80 55.40 80.80 55.40 80.80	<pre>>mpu_5f:c7:c1 cccc:10::10 mpu_5f:c7:c1 ;239.254 ccccc:10::10 '2.84.61 '2.84.61 'mpu_5f:c7:c1 'mpu_5f:c7:c1 'mpu_5f:c7:c1 '2.66808 bits), 'u_5f:c7:c1 (08: '4, Src: 10.0.2 'accl, Src Port: '00 27 5f c7 c1 '00 28 60 00 00 05 '25 14 29 24 '15 35 42 29 24 ''5 35 42 29 ''5 55 55 55 55 ''5 55 55 55 ''5 55 55 55 ''5 55 55 55 ''5 55 55 55 55 ''5 55 55 55 ''5 55 55 55 ''5 55 55 55 ''5 55 55 55 55 ''5 55 55 55 55 ''5 55 55 55 55 ''5 55 55 55 55 ''5 55 55 55 55 ''5 55 55 55 55 55 ''5 55 55 55 55 55 ''5 55 55 55 55 55 55 ''5 55 55 55 55 55 55 55 55 55 ''5 55 55 55 55 55 55 55 55 55 55 55 55</pre>	Broadcast ff02:11:ff00:1 Broadcast 10.0.2.15 ff02:11:ff00:1 10.0.2.15 Broadcast Broadcast Broadcast Broadcast Broadcast 851 bytes captured 0827:5f:c7:c1), Dst 185, 28.20. 49841, Dst Port: 80 08 00 45 00 HT - 5 64 02 50 18 c. cf 67 67	ARP ICMPv6 ARP ICMPv6 TCP ICMPv6 TCP ARP ARP ARP ARP ARP (6808 bits) ; RealtekU_1 195 ; Seq: 1, Ac	42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 86 Neighbor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 60 [TCP Retransmission] 80 + 4965 ³ [FIN, ACK] Seq=1 Ack=1 Win=65535 L 86 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 195.28.201.174 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 43 Who has 216.58.201.174 ³ Tell 192.168.70.126 44 Who has 216.58.201.174 ³ Tell 192.168.70.126 45 Who has 216.58.201.174 ³ Tell 192.168.70.126 45 Who has 216.58.201.174 ³ Tell 192.168.70.126 46 Lission (Science Content of Cont	
533 73.600 534 74.040 535 74.044 536 74.044 537 74.544 538 75.046 539 75.046 539 75.046 549 75.343 541 75.546 543 76.046 Frame 27: 85 Ethernet II, Internet Pro Transmission 1000 325 400 1010 03 45 56 1020 14 c3 c2 1030 fa fa d0 404 66 c2 fe 92	2522 PCsCo 25232 PCsCo 25279 2001: 5676 PcsCo 35579 8.248 3351 2001: 5507 52.14 3306 PcsCo 2522 PcsCo 3164 PcsCo 25484 PcsCo 3164 PcsCo 5484 PcsCo 1 bytes on wi Src: PcsComp 12 35 02 86 (55 40 08 80 45 9) 25 00 00 50 45 25 00 00 55 4	<pre>mpu_5fic7:c1 cccc:10::10 mpu_5fic7:c1 %.239.254 cccc:10::10 mpu_5fic7:c1 mpu_5fic7:c1 mpu_5fic7:c1 mpu_5fic7:c1 mpu_5fic7:c1 e (6808 bits), u_5fic7:c1(08.0; ocol, Src Port: 000 27 5f c7 c1 66 00 00 08 00 c1, Src Port: 000 27 5f c7 c1 66 00 00 08 00 c2 7 5f c7 c1 06 20 00 08 00 c2 7 5f c7 c1 06 20 00 08 00 c2 7 5f c7 c1 06 20 00 08 00 c2 7 5f c7 c1 06 20 00 08 00 c2 7 5f c7 c1 06 20 00 08 00 c2 7 5f c7 c1 06 20 00 08 00 c2 7 5f c7 c1 c2 70 68 70 20 c3 27 66 70 20 c3 27 70 63 70 20 c3 27 70 63 70 20 c3 27 70 63 70 c3 27 70 63 c3 20 27 70 63 70 c3 27 70 63 c3 20 27 70 63 c3 20 27 70 63 c3 20 20 c3 20</pre>	Broadcast ff02:1:ff00:1 Broadcast 10:0.2.15 ff02:1:ff00:1 10:0.2.15 Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Boold Strong Broadcast Broadcast Broadcast Broadcast Boold Strong Broadcast Broadcast <	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP ARP (6808 bits) : RealtekU_1 195 ; Seq: 1, AG E- P.\d.P. PO ST /logi	42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 48 Neighor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 60 [TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 86 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 195.28.201.174 ³ Tell 192.168.70.126 42 Who has 195.28.201.97 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 195.28.20.95 ³ Tell 192.168.70.126 42 Who has 195.28.20 ³ Tell 192.168.70.126 42 Who has 195.28.20 ³ Tell 192.168.70.126 42 Who has 195.28 ³ Tell 192.168.70.126 43 Who has 195.28 ³ Tell 192.168.70.126 44 Who has 195.28 ³ Tell 192.168.70.126 45 Tell 192.168 ³ Tell 192 ³ Tell 192.168 ³ Tell 192 ³ Tell	
533 73.600 534 74.044 535 74.044 536 74.546 538 75.046 538 75.046 539 75.046 539 75.046 540 75.343 541 75.546 543 76.046 Frame 27: 85 Ethennet II, Internet Pro Irransmission 600 52 54 00 10 03 45 56 201 14 c3 c2 030 fa f0 dd 040 66 2f 69 50 2f 31 2e	2322 PCsCc 2327 PCsCc 2379 2001: 5676 PCsCc 5679 8.248 3351 2001: 5507 52.14 3366 PCsCc 5222 PCsCc 3164 PCsCc 3164 PCsCc 3164 PCsCc 3164 PCsCc 35484 PCsCc 10 bytes on wi Src: PCsComp tocol Version 12 35 02 08 (51 00 50 59 52 00 00 50 66 64 65 78 : 11 0d 08 48 (<pre>mpu_5f:c7:c1 cccc:10::10 mpu_5f:c7:c1</pre>	Broadcast ff02:11:ff00:1 Broadcast 10:0.2.15 ff02:11:ff00:1 10:0.2.15 Broadcast	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP ARP C(6808 bits) : RealtekU_1 195 ; Seq: 1, AA ; Seq: 1, AA PO ST /logi ex. php HTTP Ho st: curs	42 Who has 192.168.70.254 [°] Tell 192.168.70.126 42 Who has 216.58.201.174 [°] Tell 192.168.70.126 86 Weighbor Solicitation for 2001:ccc:10::1 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 [°] Tell 192.168.70.126 86 Weighbor Solicitation for 2001:cccc:10::1 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 43 → 49059 [FIN, ACK] Seq=1 Ack=1 Win=6535 L 42 Who has 192.168.70.254 [°] Tell 192.168.70.126 42 Who has 192.168.20.195 [°] Tell 192.168.70.126 42 Who has 192.168.20.195 [°] Tell 192.168.70.126 42 Who has 192.168.20.195 [°] Tell 192.168.70.126 42 Who has 192.168.201.9174 [°] Tell 192.168.70.126 42 Who has 192.163.201.9174 [°] Tell 192.168.70.126 42 Who has 192.163.201.9174 [°] Tell 192.168.70.126 42 Who has 192.165.80.201.174 [°] Tell 192.168.70.126 42 Who has 192.658.201.174 [°] Tell 192.168.70.126 43 Who has 192.658.201.174 [°] Tell 192.168.70.126 44 Who has 192.658.201.174 [°] Tell 192.168.70.126 45 Who has 192.658.201.174 [°] Tell 192.168.70.126 46 Who has 192.658.201.174 [°] Tell 192.168.70.126 47 Who has 192.658.201.174 [°] Tell 192.168.70.126 48 Who has 192.658.201.174 [°] Tell 192.168.70.126 49 Who has 192.658.201.174 [°] Tell 192.168.70.126 40 Who has 192.658.201.174 [°] Tell 192.168.7	
533 73.60 534 74.04 535 74.54 535 74.54 536 74.54 538 75.04 538 75.04 538 75.04 538 75.04 542 75.57 543 76.04 Frame 27: 85 Ethernet II, Internet Pro Transmission 000 52 54 00 10 83 45 5e 020 14 c3 c2 03 45 5e 03 5e 03 45 5e 03	2532 PCsCc 2522 PCsCc 2579 2001: 3676 PcsCc 3677 52.44 3551 2001: 3676 PcsCc 5527 52.14 3806 PcsCc 5222 PcsCc 5484 PcsCc 5484 PcsCc 557 52.548 0 control Pcrtol 12 35 02 86 06 86 b1 00 50 952 55 00 86 6e 64 65 78 31 0d 0a 48 69 6e 66 6f 57 31 0d 0a 86	<pre>mpu_sf:c7:c1 cccc:10::10 j.239.254 ccccc:10::10 j.239.254 j.251 j.25</pre>	Broadcast ff02:11:ff00:1 Broadcast 10:0.2.15 ff02:11:ff00:1 Broadcast 00:27:5f:c7:c1), Dst: 15, Dst: 185.28.20. 49841, Dst Port: 68 00 45 00 RT··S 62 0f b9 1c -C^<@	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP (6808 bits) : RealtekU_1 195 : RealtekU_1 195 . Seq: 1, Ac . Seq: 1, Ac	42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 86 Neighbor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 60 [TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L 86 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.58.201.174 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 43 Who has 216.58.201.174 ³ Tell 192.168.70.126 44 Who has 216.58.201.174 ³ Tell 192.168.70.126 45 Who has 216.58.201.174 ³ Tell 192.168.70.126 45 Who has 216.58.201.174 ³ Tell 192.168.70.126 46 Who has 216.58.201.174 ³ Tell 192.168.70.126 47 Who has 216.58.201.174 ³ Tell 192.168.70.126 48 Who has 216.58.201.174 ³ Tell 192.168.70.126 49 Who has 216.58.201.174 ³ Tell 192.168.70.126 40 Who has 200 Tell 192.168.70 Tell 192.168.70 Tell 192.168.70 Tell 192.168.70 Tell 192.168.70 Tell 192.168.70 Tell 1	
533 73.605 534 74.046 535 74.546 535 74.546 536 74.546 538 75.046 539 75.046 539 75.046 539 75.046 542 75.578 543 76.046 Frame 27: 85 Ethernet II, Internet Pro Transmission 000 52 54 00 010 03 45 56 020 14 63 c2 030 fa f0 d0 406 6e 2f 69 050 2f 31 2e 060 6f 73 2e 066 6f 73 2e	2322 PcsCc 2523 PcsCc 2579 2001: 3676 PcsCc 3531 2001: 35507 52.14 3567 52.24 366 PcsCc 3164 PcsCc 3164 PcsCc 1 bytes on wi Src: PcsComp 12 35 02 08 6 a5 40 00 80 05 95 25 00 00 50 95 25 00 00 50 95 31 0d 0a 48 6 66 66 67 78 31 0d 0a 48 69 66 66 76 31 0d 0a 48	<pre>mpu_sfic7:c1 cccc:10::10 mpu_sfic7:c1 s.239.254 cccc:10::10 mpu_sfic7:c1 mpu_s</pre>	Broadcast ff02:1:ff00:1 Broadcast 10:0:2.15 ff02:1:ff00:1 10:0:2.15 Broadcast	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP ARP C(6808 bits) : RealtekU_1 195 ; Seq: 1, AG P.\d.P. PO ST /logi ex. php HTP Ho st: curs for activa.n on activa.n	42 Who has 192.168.70.254 ⁷ Tell 192.168.70.126 42 Who has 216.58.201.174 ⁷ Tell 192.168.70.126 48 Neighor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 ⁷ Tell 192.168.70.126 60 [TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 86 Neighor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6 42 Who has 216.58.201.174 ⁷ Tell 192.168.70.126 42 Who has 192.168.70.254 ⁷ Tell 192.168.70.126 42 Who has 185.28.201.174 ⁷ Tell 192.168.70.126 42 Who has 216.58.201.174 ⁷ Tell 192.168.70.126 42 Who has 195.28.20.95 ⁷ tell 192.168.70.126 42 Who has 195.78.70.126 42 Who has 195.78.70.126 43 Who has 195.78.70.126 44 Who has 195.78.70.126 45 Who has 195.78.70.126 46 Who has 195.78.70.126 47 Who has 195.78.70.126 48 Who has 195.78.70.126 49 Who has 195.78.70.126 40 Who has 195.78.70.126 41 Who has 195.78.70.126 42 Who has 195.78.70.126 43 Who has 195.78.70.126 44 Who has 195.78.70.126 45 Who has 195.78.70.126 46 Who has 195.78.70.126 47 Who has 195.78.70.126 48 Who has 195.78.70.126 49 Who has 195.78.70.126 40 Who has 195.78.70.126 40 Who has 195.78.70.126 40 Who has 195.78.70.127 40 Who has 195.78.70.126 40 Who has 195.78.70.127 40 Who has 195.78.70.127 40 Who has 195.7	
533 73.600 534 74.040 535 74.040 535 74.040 538 75.040 538 75.044 538 75.044 538 75.044 540 75.343 541 75.546 542 75.576 542 75.576 543 76.040 Frame 27: 85 Ethernet II, Internet Pro Transmission 000 52 54 00 010 03 45 5e 020 14 c3 c2 030 fa fo dd 040 6e 2f 69 05 74 04 05 65 75 26 05 74 06 06 56 55 74 00	2322 PCsCc 25232 PCsCc 2579 2001: 3676 PCsCc 3551 2001: 3551 2001: 3551 2001: 3551 2001: 3551 2001: 3561 2001: 5507 52:14 2607 52:14 92:22 PcsCc 30:6 PcsCc 348:4 PcsCc 10:10 PcsCc 25:00 00 25:00 00 25:00 00 20:00 05:04 20:00 05:04 20:00 05:04 20:00 05:04 20:00 05:04 60:04 43:05 00:04 36:06 20:04 06:06 20:04 06:06 20:04 06:06 20:04 06:06 20:04 06:06 20:04 06:06<	<pre>mpu_5f:c7:c1 cccc:10::10 cccc:10::10 cccc:10::10 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 mpu_5f:c7:c1 cccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 cccl.10::10 cccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 cccl.10::10 ccccl.10::10 cccl.10::10 ccccl.10::10 cccl.10::10 cccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 ccccl.10::10 cccccl.10::10 cccccl.10::10 ccccc.10::10 ccccc.10::10 ccccc.10::10 ccccc.10::10 ccccc.10::10 ccccc.10::10 cccc.10::10 ccccc.10::10 cccc.10::10 ccccc.10::10 cccc.10::10 cccc.10::10</pre>	Broadcast ff02:11:ff00:1 Broadcast 10:0.2.15 ff02:11:ff00:1 10:0.2.15 Broadcast	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP ARP C(6808 bits) : RealtekU_1 195 ; Seq: 1, AA ; Seq: 1, Context P: V	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 43 Who has 192.168.70.254? Tell 192.168.70.126 44 Who has 192.168.70.254? Tell 192.168.70.126 45 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:55:c7:c1 45 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:55:c7:c1 42 Who has 192.165.201.174? Tell 192.168.70.126 42 Who has 192.165.70.254? Tell 192.168.70.126 42 Who has 192.165.70.254? Tell 192.168.70.126 42 Who has 185.28.201.174? Tell 192.168.70.126 42 Who has 192.165.800.112:35:02) ck: 1, Len: 797	
533 73.600 534 74.040 535 74.041 535 74.041 536 74.541 538 75.041 538 75.041 538 75.041 538 75.041 543 75.542 543 76.046 Frame 27: 852 Ethernet II, Internet Pro Transmission 000 52 54 00 100 83 45 5e 020 14 c3 c2 036 fa fa dd 040 6e 2f 69 050 2f 31 2e 060 6f 73 2e 076 574 06 56 574 06 56 56 774 56 574 06 56 56 574 06 57 575 57	2532 PCSC0 2523 PCSC0 2527 2001: 3676 PCSC0 3677 52.44 3551 2001: 3567 52.24 3551 2001: 3567 52.24 3551 2001: 3567 52.24 5222 PCSC0 5223 PCSC0 52484 PCSC0 57c: PCSC0mp tocol Version Control Prot 12 35<02.86	mpu_fsic?:1 vccc:10::10 vccc:10::10 vccc:10::10 vccc:10::10 vccc:10::10 vccc:10::10 vcccc:10::10 vccccc:10::10 vccccc:10::10 vccccc:10::10 vccccc:10::10 vcccccc:10::10 vcccccc:10::10 vcccccccccccccccccccccccccccccccccccc	Broadcast ff02::1:ff00:1 Broadcast 10:0.2.15 ff02::1:ff00:1 10:0.2.15 Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast 00:2:f5:c7:c1), Dst .15, Dst: 185.28.20 49841, Dst Port: 80 08 00 45 00 62 0f b9 10: E^{-0}_{-0} 64 02 50 18 65 6f 67 69 77 27 3/1.1: 76 61 2e 6e os.im 66 67 69 43 6f 6e 74 keep-1 35 34 00 on ent_U	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP ARP (6808 bits) : RealtekU_1 195 ; Seq: 1, Ad Seq: 1, Ad P.\E- P.\E- P. ST /leg ex. php HTTP Ho st: curs for activa.n onn ection: ali ve· Cont eng th: 54-	42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 86 Neighbor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 60 [TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L 86 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.70.254 ³ Tell 192.168.70.126 42 Who has 192.168.82.201.95 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 43 Who has 216.58.201.174 ³ Tell 192.168.70.126 44 Who has 216.58.201.174 ³ Tell 192.168.70.126 45 Win has 216.58.201.174 ³ Tell 192.168.70.126 45 Who has 216.58.201.174 ³ Tell 192.168.70.126 46 Who has 216.58.201.174 ³ Tell 192.168.70.126 47 Who has 216.58.201.174 ³ Tell 192.168.70.126 48 Who has 216.58.201.174 ³ Tell 192.168.70.126 49 Who has 216.58.201.174 ³ Tell 192.168.70.126 40 Who has 216.58.201.174 ³ Tell 192.168.70.126 40 Who has 216.58.201.174 ³ Tell 192.168.70.126 40 Who has 216.58.201.174 ³ Tell 192.168.70.126 41 Who has 216.58.201.174 ³ Tell 192.168.70.126 42 Who has 216.58.201.174 ³ Tell 192.168.70.126 43 Who has 216.58.201.174 ³ Tell 192.168.70.126 44 Who has 216.58.201.174 ³ Tell 192.168.70.126 45 Who has 216.58.201.174 ³ Tell 192.168.70.126 46 Who has 216.58.201.174 ³ Tell 192.168.70.126 47 Who has 216.58.201.174 ³ Tell 192.168.70.126 48 Who has 216.58.201.174 ³ Tell 192.168.70.126 49 Who has 216.58.201.174 ³ Tell 192.168.70.126 40 Who has 200 Tell 192.168.70 ³ Tell 19	
533 73.605 534 74.044 535 74.044 536 74.544 537 74.544 538 75.044 539 75.044 539 75.044 540 75.343 541 75.546 542 75.576 543 76.046 Frame 27: 85 Ethernet II, Internet Pro Transmission 000 52 54 00 010 03 45 56 020 14 c3 c2 030 fa f0 dd 040 6e 2f 69 050 2f 31 2e 060 6f 73 2e 060 6f 75 76 060 6f 75 76	2322 PcsCc 2523 PcsCc 2579 2001: 3676 PcsCc 3531 2001: 3567 S2.24 3511 2001: 3507 S2.14 360 PcsCc 3164 PcsCc 3164 PcsCc 351 2001: 352: PcsCcomp 10 State PcsCc 11 bytes on wit Src: PcsComp 12 35 02 08 6 45 40 00 80 9 25 00 00 50 9 25 00 00 50 9 31 0d 0a 48 6 66 64 65 78: 31 0d 0a 48 69 66 66 77 31 0d 0a 48 69 66 66 56 6 70 2d 61 6cc 6 20 4 c1 65 6e 6 68 65 2d 43; 1 81 67 6; 7	<pre>mpu_sfic7:c1 cccc:10::10 mpu_sfic7:c1 s.239.254 cccc:10::10 mpu_sfic7:c1 mpu_s</pre>	Broadcast ff02:1:ff00:1 Proadcast 10:0.2.15 ff02:1:ff00:1 10:0.2.15 Broadcast	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP ARP ARP ARP C(6808 bits) : RealtekU_1 195 ; Seq: 1, Ad Content of the second Post / Logi ex. php HTP-Ho st: curs for activa.n on activa.n on activa.s ali ve-Cont trol: m g th: 54	42 Who has 192.168.70.254 ⁷ Tell 192.168.70.126 42 Who has 216.58.201.174 ⁷ Tell 192.168.70.126 86 Neighor Solicitation for 2001:ccc:10:11 from 08:00:27:5f:c7:c1 42 Who has 192.168.70.254 ⁷ Tell 192.168.70.126 60 [TCP Retransmission] 80 + 49695 [FIN, ACK] Seq=1 Ack=1 Win=65535 L. 86 Neighor Solicitation for 2001:cccc:10:11 from 08:00:27:5f:c7:c1 132 [TCP Retransmission] 443 → 49741 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6 42 Who has 216.58.201.174 ⁷ Tell 192.168.70.126 42 Who has 192.168.70.254 ⁷ Tell 192.168.70.126 42 Who has 192.168.70.254 ⁷ Tell 192.168.70.126 42 Who has 185.28.201.174 ⁷ Tell 192.168.70.126 42 Who has 216.58.201.174 ⁷ Tell 192.168.70.126 43 Who has 216.58.201.174 ⁷ Tell 192.168.70.126 44 Who has 216.58.201.274 ⁷ Tell 192.168.70.126 45 Who has 216.58.201.174 ⁷ Tell 192.168.70.126 46 L235:02 (52:54:00:12:35:02) 47 Tell 192 Tell 192.168.70.126	
533 73.600 534 74.044 535 74.044 535 74.044 538 75.044 538 75.044 538 75.044 538 75.044 540 75.345 542 75.576 542 75.576 542 75.577 543 76.046 Frame 27: 85 Ethernet II, Internet Pro Transmission 600 52 54 00 61 03 45 5e 620 14 c3 c2 63 fa fo 64 65 65 65 67 74 66 66 65 65 67 32 66 60 66 17 8 22 60 43 61 63 60 60 17 8 20 60 43 61 63 60 60 17 8 20 61 78 20 60 43 61 63 60 60 17 8 20 60 43 61 63 50 60 17 8 20 60 43 61 63 50 60 17 8 20 51 76 65 51 76 65 51 76 76 52 56 76 52 56 76 53 76 76 54 56 56 54 57 56 56 77 57 57 57 56 57 56 57	232 PCsCc 2329 PCsCc 2379 2001: 5676 PCsCc 5679 8.248 5517 52.14 2001: 5507 52.14 2001: 5507 52.14 2001: 5507 52.14 PCsCc 13360 PCsCc 5222 PCsCc 1364 PCsCc 5222 PCsCc 1364 PCsCc 5222 PCsCc 14 PCsCc 14 PCsCc 15	<pre>mpu_sf:c7:c1 cccc:10::10 mpu_sf:c7:c1</pre>	Broadcast ff02:11:ff00:1 Broadcast 10:0.2.15 ff02:11:ff00:1 10:0.2.15 Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast 00:27:5f:c7:c1), Dst 10:5 Dst: 185:28.20. 49841, Dst Port: 80 68 00 45 00 RT-5 02 of b9 1c 64 02 50 18 65 67 69 67 73 71.1. 76 61 2e 6e 63 75 72 71.1. 76 61 2e 30 et -C(C) 43 6f 6e 74 62 32 00 et-C(C) 63 6 70 69 ed 63 75 72 73.1. 73 64 73 20 et-C(C)	ARP ICMPv6 ARP TCP ICMPv6 TCP ARP ARP ARP ARP ARP ARP C(6808 bits) : RealtekU_1 195 (6808 bits) : RealtekU_1 195 (5809 bits) : RealtekU_1 195 (5809 bits) : RealtekU_1 195 (5809 bits) : RealtekU_1 195 (5809 bits) : RealtekU_1 195 (5809 bits) : RealtekU_1 : Content :	42 Who has 192.168.70.254? Tell 192.168.70.126 42 Who has 216.58.201.174? Tell 192.168.70.126 43 Who has 192.168.70.254? Tell 192.168.70.126 44 Who has 192.168.70.254? Tell 192.168.70.126 45 Neighbor Solicitation for 2001:cccc:10:11 from 08:00:27:57:c7:c1 42 Who has 192.165.8.201.174? Tell 192.168.70.126 42 Who has 192.165.70.254? Tell 192.168.70.126 42 Who has 192.165.8.201.174? Tell 192.168.70.126 42 Who has 185.28.20.195? Tell 192.168.70.126 42 Who has 185.28.20.195? Tell 192.168.70.126 42 Who has 185.28.201.174? Tell 192.168.70.126 42 Who has 192.165.8.201.174? Tell 192.168.70.126 42 Who has 195.8.201.174? Tell 192.168.70.126 42 Who has 195.754:00:12:35:02) 53 0 (52:54:00:12:35:02) 54 1, Len: 797	

Desde el ordenador amenazado (PC3 – Windows/Linux):

a) Cerrar o abrir puertos (Windows y Linux).

b) Realiza un informe sobre software anti-sniffers Y SI LO CONSIDERAS NECESARIO UTILIZA EL MISMO para detectar desde PC3 sniffers situados en la red.

Vamos a bloquear el puerto 139 para ver si el equipo atacante no consigue localizarlo. Para ello crearemos una nueva regla de entrada y de salida bloqueado el puerto.



Escogemos TCP y el puerto.

🔐 Asistente para nueva regla de entrada 🗾 🗾							
Protocolo y puertos							
Especifique los puertos y protocolos a los que se aplica esta regla.							
Pasos:							
Tipo de regla	¿Se aplica esta regla a TCP o UDP?						
Protocolo y puertos O TCP							
 Acción 	Acción OUDP						
 Perfil 							
 Nombre 	¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?						
	Todos los puertos locales						
	Puertos locales específicos: 139						
	Ejemplo: 80, 443, 5000-5010						
	Más información acerca de protocolos y puertos						
	Atrás Siguiente > Cancelar						

Lo bloquearemos.



Perfil	
specifique los perfiles en los q	ue se va a aplicar esta regla.
Tipo de regla	¿Cuándo se aplica esta regla?
Acción	☑ Dominio Se aplica cuando un equipo está conectado a su dominio corporativo.
Nombre	 Privado Se aplica cuando un equipo está conectado a una ubicación de redes privadas. Público
	Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

Le pondremos un nombre.

Pasos: • Tipo de regla • Protocolo y puertos • Acción • Perfil • Nombre: p2	Nombre Especifique el nombre y la desc	ipción de esta regla.	
 Tipo de regla Protocolo y puertos Acción Perfil Nombre: p2 	Pasos:		
Protocolo y puertos Acción Perfil Nombre: p2	Tipo de regla		
Acción Perfil Nombre: p2	Protocolo y puertos		
Perfil Nombre: p2	Acción		
P2	Perfil	Nombre:	
	Nombre	p2	
Descripción (opcional):		Descripción (opcional):	

Nos deberá quedar una cosa tal que así:

Firewall de Windows con segur	Reglas de entrada			
🔣 Reglas de entrada	Nombre	Grupo	Perfil	Habilit
Reglas de seguridad de con	⊘ p2		Todo	Sí
Supervisión	Administración remota de Firewall de Wi	Administración remota de F	Domi	No
	Administración remota de Firewall de Wi	Administración remota de F	Priva	No
	Administración remota de Firewall de Wi	Administración remota de F	Priva	No
	Madministración remota de Firewall de Wi	Administración remota de F	Domi	No

Firewall de Windows con segur	Reglas de salida				
Reglas de entrada	Nombre	Grupo	Perfil	Habilitado	-
Reglas de seguridad de con	O 02		Todo	Sí	
Supervisión	🔘 Asistencia remota (PNRP de salida)	Asistencia remota	Público	No	
	🕖 Asistencia remota (PNRP de salida)	Asistencia remota	Domi	Sí	
	🕢 Asistencia remota (SSDP-TCP de salida)	Asistencia remota	Domi	Sí	Ε
	🔇 Asistencia remota (SSDP-UDP de salida)	Asistencia remota	Domi	Sí	
	🕑 Asistencia remota (TCP de salida)	Asistencia remota	Domi	Sí	
	🜑 Asistencia remota (TCP de salida)	Asistencia remota	Público	No	

Vemos como dicho puerto ya no aparece abierto.

👁 Zenmap		
Esc <u>a</u> neo Herramien <u>t</u> as <u>F</u>	terfil Ayuda (<u>H</u>)	
Objetivo: 192.168.70.82	▼ Perfil:	Escaneo Cancelar
Comando: nmap -T4 -F 1	92.168.70.82	
Servidores Servicios	Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos	Detalles
III 192.168.70.81 III 192.168.70.82 III 192.168.70.126	Starting Nmap 7.80 (https://nmap.org) at 2019-10-09 13:30 Hora de verano romance Nmap scan report for 192.168.70.82 Host is up (0.12s latency). Not shown: 99 filtered ports PORT STATE SERVICE 5357/tcp open usdapi MAC Address: 7C:2A:31:5F:E8:FA (Intel Corporate)	
	Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds	-

Para volver a abrirlo solo tendremos que eliminar la regla.



Después de eliminar la regla volveremos a ver como aparece de nuevo el puerto abierto.

👁 Zenmap						
Esc <u>a</u> neo Herramien <u>t</u> as <u>P</u>	erfil Ayuda (<u>H</u>)					
Objetivo: 192.168.70.82	Perfil:	Escaneo Cancelar				
Comando: nmap -p 1-1023 192.168.70.82						
Servidores Servicios	Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos					
OS ◀ Servidor ▲	nmap -p 1-1023 192.168.70.82	▼ Detalles				
 192.168.70.81 192.168.70.82 192.168.70.126 	Starting Nmap 7.80 (https://nmap.org) at 2019-10-09 13:40 Hora de verano romance Nmap scan report for 192.168.70.82 Host is up (0.014s latency). Not shown: 1020 closed ports PORT STATE SERVICE 135/tcp open msrpc 135/tcp open metbios-ssn 445/tcp open mitrosoft-ds MAC Address: 7C:2A:31:5F:EB:FA (Intel Corporate)					
	Nmap done: 1 IP address (1 host up) scanned in 38.49 seconds	-				

Lo siguiente será realizar lo mismo, pero en Ubuntu. Abriremos el puerto 80 y 8080.

Con *nmap -p [rango puertos] [IP]* podremos buscar por rango de puertos. Vemos que no hay ningún puerto abierto.

🗢 Zenmap	
Esc <u>a</u> neo Herramien <u>t</u> as <u>P</u> erfil Ayuda (<u>H</u>)	
Objetivo: 192.168.70.130 💌 Perfil:	▼ Escaneo Cancelar
Comando: nmap -p 1-1023 192.168.70.130	
Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del s	ervidor Escaneos
OS • Servidor nmap-p1-1023192.168.70.130 W 192.168.70.81 Starting Nmap 7.80 (https://nmap.org) at 2015 W 192.168.70.126 Starting Nmap 7.80 (https://nmap.org) at 2015 W 192.168.70.126 Map scan report for 192.168.70.130 W 192.168.70.130 Host is up (0.005 lattency). Map scan report for 192.168.70.130 Host is up (0.005 lattency). Map scan report for 192.168.70.130 are cl MAC Address: 08:00:27:68:C3:C8 (Oracle Virtuals Map done: 1 IP address (1 host up) scanned in Map done: 1 IP address (1 host up) scanned in	►10-09 14:18 Hora de verano romance osed iox virtual NIC) 0.39 seconds
Filtrar servidores	

Abriremos el puerto 80 y 8080.

sudo ufw allow 80

sudo ufw allow 8080

```
franciscojesus@sri-ubuntu18-practicas:~$ sudo ufw allow 80
[sudo] contraseña para franciscojesus:
Regla añadida
Regla añadida (v6)
franciscojesus@sri-ubuntu18-practicas:~$ sudo ufw allow 8080
Regla añadida
Regla añadida (v6)
franciscojesus@sri-ubuntu18-practicas:~$ sudo ufw reload
```

```
El cortafuegos se ha recargado
<mark>franciscojesus@sri-ubuntu18-practicas:</mark>~$ sudo ufw allow 443
Regla añadida
Regla añadida (v6)
```

También lo podremos hacer con IPTables.

franciscojesus@sri-ubuntu18-practicas:~\$ sudo iptables -A INPUT -p tcp -d 0/0 -s 0/0 --dport 8080 -j ACCEPT

Vemos que en *State* aparece como *Closed,* esto ocurre porque en Ubuntu, todos los puertos se abren a menos que tenga un firewall o una aplicación que lo esté bloqueando. En circunstancias normales, la aplicación que se ejecuta en el puerto es para escuchar.

Un puerto generalmente se considera abierto cuando hay un programa ejecutándose y escuchando en el puerto.

Como vemos hemos abierto el puerto http y http-proxy.

Zenmap					
Esc <u>a</u> neo Herramien <u>t</u> as <u>F</u>	2erfil Ayuda (<u>H</u>)				
Objetivo: 192.168.70.130	Perfil: Quick scan Cancelar				
Comando: nmap - T4 - F 192.168.70.130					
Servidores Servicios OS 4 Servidor II 192.168.70.81 III II 192.168.70.82 IIII III 192.168.70.126 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos nmap -T4 -F192.168.70.130 Imap -T4 -F192.168.70.130 Imap -T4 -F192.168.70.130 Imap -Scan report for 192.168.70.130 Imap -Scan report for 192.168.70.100 Imap -Scan report for 192.100 Imap -Scan r				

Hemos cerrado el puerto MySQL y hemos abierto el https (443).

sudo ufw dwny 3306

🌣 Zenmap						
Esc <u>a</u> neo H	lerramien <u>t</u> as <u>P</u>	erfil Ayuda (H)				
Objetivo:	192.168.70.130	Perfil: Quick scan	•			
Comando:	nmap - T4 - F 19	92.168.70.130				
Servidores	Servicios	Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos				
OS 4 Servid	lor 🔺	nmap - T4 - F 192.168.70.130				
■ 192.10	68.70.130	<pre>Starting Nmap 7.80 (https://nmap.org) at 2019-10-09 18:32 Hora de verano romance Nmap scan report for 192.168.70.130 Host is up (0.00066s latency). Not shown: 97 filtered ports PORT STATE SERVICE 80/tcp closed http 443/tcp closed https 8080/tcp closed https</pre>				

*Nota: Puede que en algún momento tengamos que reiniciar UFW o IPTABLES.

sudo ufw disable sudo ufw enable

sudo service iptables restart

Informe sobre Anti-Sniffer

¿Qué es y para qué sirve ARP?

En una red Ethernet cuando queremos enviar un paquete IP entre dos hosts conectados las únicas direcciones válidas son las MAC y lo que circula son tramas Ethernet. Entonces y volviendo al ejemplo de antes cuando queremos enviar un paquete IP lo que se hace es meter el paquete dentro de una trama Ethernet y enviar.

¿Cuál es el problema entonces?

El problema radica en que sabemos la dirección IP del host de destino, pero no su dirección MAC.

¿Cómo se soluciona esto?

La solución está en que antes de enviar el paquete IP se debe usar ARP para averiguar cuál es la dirección MAC del host destino de la conexión que pretendemos realizar.

Las técnicas de detección.

El test DNS

En este método, la herramienta de detección en sí misma está en modo promiscuo. Creamos numerosas conexiones TCP falsas en nuestro segmento de red, esperando un sniffer pobremente escrito para atrapar estas conexiones y resolver la dirección IP de los inexistentes hosts. Algunos sniffers realizan búsquedas inversas DNS en los paquetes que capturan. Cuando se realiza una búsqueda inversa DNS, una utilidad de detección de sniffers "huele" la petición de las operaciones de búsqueda para ver si el objetivo es aquel que realiza la petición del host inexistente.

El Test del Ping

Este método confía en un problema en el núcleo de la máquina receptora. Podemos construir una petición tipo "ICMP echo" con la dirección IP de la máquina sospechosa de hospedar un sniffer, pero con una dirección MAC deliberadamente errónea. Enviamos un paquete "ICMP echo" al objetivo con la dirección IP correcta, pero con una dirección de hardware de destino distinta. La mayoría de los sistemas desatenderán este paquete ya que su dirección MAC es incorrecta. Pero en algunos sistemas Linux, NetBSD y NT, puesto que el NIC está en modo promiscuo, el sniffer asirá este paquete de la red como paquete legítimo y responderá, por consiguiente.

Si el blanco en cuestión responde a nuestra petición, sabremos que está en modo promiscuo. Un atacante avanzado puede poner al día sus sniffers para filtrar tales paquetes para que parezca que el NIC no hubiera estado en modo promiscuo.

El Test ICMP

En este método, hacemos ping al blanco y anotamos el Round Trip Time (RTT, retardo de ida y vuelta o tiempo de latencia). Creamos centenares de falsas conexiones TCP en nuestro segmento de red en un período de tiempo muy corto. Esperamos que el sniffer esté procesando estos paquetes a razón de que el tiempo de latencia incremente. Entonces hacemos ping otra vez, y comparamos el RTT esta vez con el de la primera vez. Después de una serie de tests y medias, podemos concluir o no si un sniffer está realmente funcionando en el objetivo o no.

El test ARP

Podemos enviar una petición ARP a nuestro objetivo con toda la información rápida excepto con una dirección hardware de destino errónea. Una máquina que no esté en modo promiscuo nunca verá este paquete, puesto que no era destinado a ellos, por lo tanto, no contestará. Si una máquina está en modo promiscuo, la petición ARP sería considerada y el núcleo la procesaría y contestaría. Por la máquina que contesta, la sabemos estamos en modo promiscuo.

El test Etherping

Enviamos un "ping echo" al host a testear con una IP de destino correcta y dirección MAC falseada. Si el host responde, es que su interfaz está en modo promiscuo, es decir, existe un sniffer a la escucha y activo.

Protegerse contra la acción de los sniffers

A grandes rasgos para protegernos de los sniffers y para que éstos no cumplan sus objetivos de olfateo de contraseñas y en general nos "lean datos sensibles" en texto plano -sin cifrado fuerte, podemos hacer uso de diversas técnicas o utilizar sistemas como:

- o Redes conmutadas (no siempre es efectivo)
- o PGP
- o SSL
- o SSH
- o VPN
- o etc.

Conclusión

La práctica ha sido muy entretenida en conjunto con mi compañero Alex Valdepeñas, ha sido muy curioso ser uno el atacante y otro la victima y realizar el ataque mint. Prácticas así se aprende y entretiene uno realmente. En la práctica hemos podido realizar muchas cosas interesantes también como abrir y cerrar puertos en Windows y Linux o ataques de reconocimiento. Muy chula está práctica en grupos de 2.