Sumario

UΤ	02 – Apéndice: Exploradores de red	2
	Introducción a las herramientas de red	2
	Explorar un segmento de red: nmap	2
	Explorar el propio sistema: netstat	3
	Análisis avanzado: wireshark (anteriormente ethereal)	5
	Tutoriales y ejemplos de análisis de redes	7



UT 02 – Apéndice: Exploradores de red

Introducción a las herramientas de red

Este apéndice se incluye en la Unidad de Trabajo como material adicional (de estudio no obligatorio) para proporcionar al alumno información y herramientas relacionadas con la administración de redes.

Para obtener información acerca del comportamiento de un sistema, redes de comunicaciones, puertos abiertos, otros equipos conectados a la red, etc... se utilizan diferentes herramientas. Veamos algunas de ellas.

Explorar un segmento de red: nmap

El siguiente artículo muestra algunos ejemplos de uso de la herramienta nmap:

http://rm-rf.es/nmap-linux-uso-ejemplos/

Por ejemplo, para mostrar los puertos disponibles en un equipo:

```
$ nmap 192.168.0.219
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-09 18:45 CET
Nmap scan report for Audax (192.168.0.219)
Host is up (0.00013s latency).
Not shown: 993 closed ports
        STATE SERVICE
PORT
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
        open microsoft-ds
445/tcp
2049/tcp open nfs
10000/tcp open snet-sensor-mgmt
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Mostrar las rutas e interfaces de red de un equipo:



CFGM: Sistemas Microinformáticos y Redes Módulo: SERVICIOS EN RED – Curso: 2º – 2019/2020

Explorar el propio sistema: netstat

La herramienta netstat proporciona información del propio sistema en el que se ejecuta, como conexiones abiertas, puertos, etc...

https://www.linux-party.com/29-internet/8969-20-comandos-netstat-para-administradores-de-redeslinux

Por ejemplo, para ver los puertos activos:

\$ nets	tat -at									
Conexiones activas de Internet (servidores y establecidos)										
Proto	Recib En	viad	Dirección local	Dirección remota	Estado					
tcp	Θ	0	localhost:mysql	0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:netbios-ssn	0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:41131	0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:39213	0.0.0:*	ESCUCHAR					
tcp	Θ	0	localhost:24271	0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:sunrpc	0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:webmin	0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:33173	0.0.0:*	ESCUCHAR					
tcp	Θ	0	localhost:domain	0.0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:ssh	0.0.0.0:*	ESCUCHAR					
tcp	Θ	0	localhost:ipp	0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:db-lsp	0.0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:microsoft-ds	0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:41021	0.0.0:*	ESCUCHAR					
tcp	Θ	0	localhost:17600	0.0.0.0:*	ESCUCHAR					
tcp	Θ	0	0.0.0.0:nfs	0.0.0.0:*	ESCUCHAR					
tcp	Θ	0	localhost:51235	0.0.0:*	ESCUCHAR					
tcp	Θ	0	localhost:17603	0.0.0.0:*	ESCUCHAR					
tcp	Θ	0	Audax:39326	213.229.137.37:imap2	CLOSE_WAIT					
tcp	Θ	0	localhost:43250	localhost:51235	TIME_WAIT					
tcp	1	0	Audax:46316	ec2-52-203-89-21.:https	CLOSE_WAIT					
tcp	Θ	0	Audax:60260	wa-in-f109.1e100.:imaps	ESTABLECIDO					

Estadísticas por protocolo:

```
$ netstat -s
Ip:
Forwarding: 2
131905 total packets received
1 with invalid addresses
0 forwarded
0 incoming packets discarded
126382 incoming packets delivered
114337 requests sent out
22 outgoing packets dropped
3 dropped because of missing route
```



CFGM: Sistemas Microinformáticos y Redes Módulo: SERVICIOS EN RED – Curso: 2º – 2019/2020

Icmp: 1921 ICMP messages received 1012 input ICMP message failed histograma de entrada ICMP: destination unreachable: 1082 echo requests: 839 1892 ICMP messages sent 0 ICMP messages failed histograma de salida ICMP: destination unreachable: 1053 echo replies: 839 IcmpMsg: InType3: 1082 InType8: 839 OutType0: 839 OutType3: 1053 Tcp: 6563 active connection openings 1014 passive connection openings 2019 failed connection attempts 466 connection resets received 18 connections established 77693 segments received 91235 segments sent out 214 segments retransmitted 0 bad segments received 3399 resets sent Udp: 75158 packets received 43 packets to unknown port received 0 packet receive errors 25297 packets sent 0 receive buffer errors 2 send buffer errors IgnoredMulti: 716



UT 01

Análisis avanzado: wireshark (anteriormente ethereal)

Para poder usar la herramienta wireshark hay que tener permisos suficientes, además de cumplir con la legislación oportuna. Podría ser ilegal realizar ciertas operaciones de análisis de red con esta herramienta.

El siguiente artículo es una pequeña introducción a la instalación y uso de wireshark:

https://geekytheory.com/curso/wireshark/instalar-wireshark

Si queremos usar esta herramienta con un usuario diferente de root hay que darle permisos, añadíéndolo al grupo "wireshark":

\$ usermod -a -g wireshark jose

Existe una utilidad similar, en modo comando: **tshark** (hay que ejecutarla como root, mediante "sudo tshark").

Veamos un ejemplo sobre la captura de las tramas en una red durante una conexión HTTP no segura. En este ejemplo se ve cómo la contraseña del usuario viaja sin encriptar por la red, y por tanto se podría capturar con una herramienta como wireshark:

Ψ				*wlo1 (tcp port http) 🛛 📲 🖉 📩 🚄 👘 💥 Ac	olicaciones 🛛
File E	dit View Go Capture Analyze Statistic	s Telephony Tools I Q <> >	Internals Help		_
Filter:		▼ Expr	ession Clear	Apply Guardar	
No.	Time Source D	Destination	Protocol Le	ngth Info	_
5	4 10.52499675! 192.168.0.219 2	13.229.137.12	TCP	66 43584 → 80 [ACK] Seq=690 Ack=2513 Win=63104 Len=0 TSval=2546868078 TSecr=1218914668	
5	5 10.525035091 213.229.137.12 1	92.168.0.219	TCP	1835 80 - 43584 [PSH, ACK] Seq=2513 Ack=690 Win=11520 Len=969 TSval=1218914668 TSecr=2546867769 [TCP segment of a reassembled PDU]	
5	5 10.525052899 192.168.0.219 2	13.229.137.12	TCP	66 43584 → 80 [ACK] Seq=690 ACk=3482 Win=52208 Len=0 TSval=2546868078 TSecr=1218914668	
5	8 10.525074477215.229.157.12 1	13.229.137.12	TCP	1300 00 - 43304 [F35], ACK] SEC-3402 ACK-090 MILE-11220 EET-1440 ISVAE-12120314000 ISECT-2240007/09 [ICP Segment of a reassembled PD0] 56 43584 - 88 [ACK] Son=500 ACK-4922 Win-68080 [Jone TSva]=2546868087 TSecr=21389[4668	
5	9 10.52510472; 213.229.137.12 1	92.168.0.219	TCP	643 80 → 43584 [PSH, ACK] Seq=4922 Ack=690 Win=11520 Len=577 TSval=1218914668 TSecr=2546867769 [TCP segment of a reassembled PDU]	
6	0 10.525116358 192.168.0.219 2	13.229.137.12	TCP	66 43584 → 80 [ACK] Seq=690 Ack=5499 Win=60288 Len=0 TSval=2546868078 TSecr=1218914668	
6	1 10.54218635(213.229.137.12 1	92.168.0.219	TCP	442 80 - 43584 [PSH, ACK] Seq=5499 Ack=690 Win=11520 Len=376 TSval=1218914697 TSecr=2546868077 [TCP segment of a reassembled PDU]	
6	2 10.54223733 192.168.0.219 2	13.229.137.12	TCP	66 43584 → 80 [ACK] Seq=690 Ack=5875 Win=63104 Len=0 TSvat=2546868095 TSecr=1218914697	
6	4 10.55356854: 192.168.0.219 2	13.229.137.12	TCP	00 min/1.1 200 WK (LEXL/ILEL) 66 43584 - 88 (ACK) Some500 Arke5895 Win=64128 Lene0 TSva]=2546868107 TSecr=1218914699	
6	5 15.39092403 192.168.0.219 2	13.229.137.12	HTTP	1122 POST /portal/index.php?option=com users&task=user.login&Itemid=83⟨=es HTTP/1.1 (application/x-www-form-urlencoded)	
6	5 15.463326848 213.229.137.12 1	92.168.0.219	TCP	68 80 → 43584 [ACK] Seq=5895 Ack=1746 Win=17280 Len=0 TSval=1218915926 TSecr=2546872944	
6	7 15.52044256: 213.229.137.12 1	192.168.0.219	TCP	564 80 → 43584 [P5H, ACK] Seq=5895 Ack=1746 Win=17280 Len=498 TSval=1218915943 TSecr=2546872944 [TCP segment of a reassembled PDU]	
6	8 15.528486448 192.168.0.219 2	13.229.137.12	TCP	66 43584 → 80 [ACK] Seq=1746 Ack=6393 Win=63744 Len=0 TSval=2546873074 TSecr=1218915943	0
7	9 15.520595457 192.100.0.219 2	92.168.0.219	HTTP	829 GET / portar/index.php/toption-com_internationalaroview-iistariemiu-owacang-es-min/1.1 38 HTTP/1.1 303 See other (text/html) (text/html)	
7	1 15.53349899: 192.168.0.219 2	13.229.137.12	тср	66 43584 → 80 [ACK] Sec=1746 Ack=6413 Win=64128 Len=0 TSval=2546873087 TSecr=1218915943	
7	2 15.60555071; 213.229.137.12 1	92.168.0.219	TCP	68 80 → 43586 [ACK] Seq=1 Ack=764 Win=11520 Len=0 TSval=1218915961 TSecr=2546873080	
7	3 15.950735847 213.229.137.12 1	92.168.0.219	TCP	1506 80 → 43586 [PSH, ACK] Seq=1 Ack=764 Win=11520 Len=1440 TSval=1218916038 TSecr=2546873080 [TCP segment of a reassembled PDU]	
7	4 15.95079083: 192.168.0.219 2	13.229.137.12	TCP	66 43586 - 80 (ACK) Seq=764 ACk=1441 Win=63104 Len=0 TSval=2546873504 TSecr=1218916038	U
7:	5 15.95112573, 213.229.137.12 1 5 15 051150656 102 168 0 210 2	192.108.0.219	TCP	LH3 80 → 45280 [P5H, ACK] Sed=1441 ACK=/04 WLN=115/20 Lenen Tsual=10// ISVaE12128910438 ISECT=25408/39808 [ICP Segment of a reassembled PDU] 66 43586 - 88 [ACK] Som=764 Ack=2518 Winn=3144 Lenen Tsual=2548432564 TSor=T=213801638	
7	7 15.95119460 213.229.137.12 1	92.168.0.219	TCP	00 43500 4 050 [RKK] 544-104 RK+2518 AK=7518 AK=754 Kinel52 Len=983 TSval=1218916083 TSecr=2546873680 [TCP segment of a reassembled PDU]	
7	8 15.951212328 192.168.0.219 2	13.229.137.12	TCP	66 43586 → 80 [ACK] Seq=764 Ack=3501 Win=62208 Len=0 TSval=2546873504 TSecr=1218916038	
▶ Fram	e 65: 1122 bytes on wire (8976 bits),	1122 bytes captured	(8976 bits)	n interface 0	
Ethe	rnet II, Src: IntelCor_f5:13:ce (d4:2	5:8b:f5:13:ce), Dst:	AskeyCom_91:	31:f7 (d4:7b:b0:91:81:f7)	
Inte	rnet Protocol Version 4, Src: 192.168	.0.219, Dst: 213.229	1.137.12	x 5905 Jon. 1055	
Hype	rtext Transfer Protocol	45564, DSt POIL: 60,	364: 030, AC	: 3533, Leii: 1030	
▶ HTML	Form URL Encoded: application/x-www-	form-urlencoded			
0350 0	1 38 66 35 33 37 32 32 39 65 63 61 3 1 66 35 37 65 32 30 37 65 62 3d 63 6	37 30 33 65 a81537. 56 65 36 38 af57e2	22 9eca703e 87 eb=cfe68		
0370 6	3 62 65 35 65 30 37 36 62 30 31 63 3	31 32 66 61 cbe5e0	76 b01c12fa		
0380 3	10 32 64 36 63 39 37 38 30 36 62 3b 2	20 38 62 31 02d6c9	78 06b; 8b1		
0390 3	8 64 34 35 32 62 62 31 39 65 34 31 3	34 65 37 33 8045201 31 3d 65 73 ec4a6e	b1 9e414e73 35 39921=es		
03b0 2	d 45 53 0d 0a 0d 0a 75 73 65 72 6e 6	51 6d 65 3d -ES	.u sername=		
03c0 6	a 61 6a 69 6d 65 6e 65 7a 26 70 61 7	73 73 77 6f jajimer	ne z&passwo		
0300 7	2 64 30 4a 41 4a 50 72 6† 66 65 30 3 4 75 72 6e 3d 61 57 35 6b 5a 58 67 7	30 20 /2 05 Fd=	w5 kZXqucGb		
03f0 7	7 50 32 39 77 64 47 6c 76 62 6a 31 6	5a 62 32 31 wP29wd	Gl vbj1jb21		0
0400 6	i6 61 57 35 30 5a 58 4a 75 59 57 78 6	ia 59 57 78 faW50Z	XJ uYWxjYWx		
0410 0	ic 62 60 52 68 63 69 5a 32 61 57 56 3 10 63 33 51 6d 53 58 52 6c 62 57 6c 6	33 50 57 78 lbmRhc 3b 50 54 67 _pc30mS	12 2awv3PWx XR_lbWlkPTg		
0 💅	File: "/tmp/wireshark_wlo1_2019 Packets	: 92 · Displayed: 92 (100,0	%) · Dropped: 0 (0	0%)	Profi
_					



Ahora veamos un ejemplo de captura de tramas durante el proceso de asignación de parámetros de red por DHCP:

Paso 1: DHCP DISCOVER

2059 80.7119260000.0.0.0	255.255.255.255	DHCP	68	67	DHCP Discover	- Transaction ID 0x184b8a2
2060 80.716094000 192.168.1.1	192.168.1.15	DHCP	67	66	DHCP Offer	- Transaction ID 0x184b8a2
2061 80.7168230000.0.0.0	255.255.255.255	DHCP	80	67	DHCP Request	- Transaction ID 0x184b8a2
2073 81.723724000 192.168.1.1	192.168.1.15	DHCP	67	68	DHCP ACK	- Transaction ID 0x184b8a2
2665 85.4993850000.0.0.0	255.255.255.255	DHCP	68	67	DHCP Request	- Transaction ID 0x46cldf4d

Frame 2059: 342 bytes on wire (2736 bite), 342 bytes captured (2736 bits) on interface 0 Ethernet II, Src: LctcHete 46:90:e3 (68:17:28:46:96:e3), Dst: Broadcast (ff:ff:ff:ff:ff:ff). Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255) User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67) Bootstrap Protocol (Discover)

Paso 2: DHCP OFFER

2059 80.711926006 0.0.0.0 255.255.255 DHCP 68 67 <u>DHCP Discov</u> er - Tr	Transaction ID 0x184b8a2
2060 80.716094006 192.168.1.1 192.168.1.15 DHCP 67 68 DHCP Offer - Tr	Transaction ID 0x184b8a2
2061 80.716823006 0.0.0 255.255.255 DHCP 68 67 DHCP Request - Tr	Transaction ID 0x184b8a2
2073 81.723724006 192.168.1.1 192.168.1.15 DHCP 67 68 DHCP ACK - Tr	Transaction ID 0x184b8a2
2665 85.4993850060.0.0.0 255.255.255 DHCP 68 67 DHCP Request - Tr	Transaction ID 0x46c1df4d

>Frame 2060: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
>Ethernet II, Src: Netgear_90:23:7b (a0:21:b7:90:23:7b), Dst: LcfcHefe_46:96:e3 (68:f7:28:46:96:e3)
>Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.15 (192.168.1.15)
>User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
D Bootstrap Protocol (Offer)

Paso 3: DCHP REQUEST

2059 80.7119260000.0.0.0	255.255.255.255	DHCP	68	67	DHCP Discover - Transaction ID 0x184b8a2
2060 80.716094000 192.168.1.1	192.168.1.15	DHCP	67	68	DHCP Offer - Transaction ID 0x184b8a2
2061 80.7168230000.0.0.0	255.255.255.255	DHCP		67	DHCP Request - Transaction ID 0x184b8a2
2073 81.723724000 192.168.1.1	192.168.1.15	DHCP	67	68	DHCP ACK - Transaction ID 0x184b8a2
2665 85.4993850000.0.0.0	255.255.255.255	DHCP	68	67	DHCP Request - Transaction ID 0x46c1df4

Frame 2061: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface 0
Ethernet II, Src: LcfcHefe_46:96:e3 (68:f7:28:46:96:e3), Dst: Broadcast (ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Bootstrap Protocol (Request)

Paso 4: DHCP ACK

2059 80.7119260000.0.0.0	255.255.255.255	DHCP	68	67	DHCP Discover	- Transaction	ID	0x184b8a2
2060 80.716094000 192.168.1.1	192.168.1.15	DHCP	67	68	DHCP Offer	- Transaction	ID	0x184b8a2
2061 80.7168230000.0.0.0	255.255.255.255	DHCP	68	67	DHCP Request	- Transaction	ID	0x184b8a2
2073 81.723724000 192.168.1.1	192.168.1.15	DHCP	67	68	DHCP ACK	- Transaction	ID	0x184b8a2
2665 85.4993850000.0.0.0	255.255.255.255	DHCP	68	67	DHCP Request	- Transaction	ID	0x46c1df4d

Frame 2073: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_90:23:7b (a0.21:b7:90:23:7b), Dst: LcfcHefe_46:96:e3 (68:f7:28:46:96:e3)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.15 (192.168.1.15)
User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
Bootstrap Protocol (ACK)



Tutoriales y ejemplos de análisis de redes

Para finalizar, enlazamos algunos artículos relacionados con herramientas de análisis de red: https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-losdatos/ https://seguridadyredes.wordpress.com/2008/04/30/tshark-wireshark-en-linea-de-comandos-i-parte/ Y aquí tenemos dos artículos más, relativos al uso de nmap y netstat:

https://infosegur.wordpress.com/unidad-5/servicios-de-red-nmap-y-netstat/

https://superuser.com/questions/1065478/what-is-the-difference-between-nmap-and-netstat

