



Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: ING. Edgar Martínez Meza

Asignatura: Laboratorio de Redes de datos seguras

Grupo: 6

No de Práctica(s): # 6

Integrante(s): Barrera Peña Víctor Miguel

Tapia Escobar José Alejandro


*No. de Equipo de
cómputo empleado:* #3


Semestre: 2024 - 2

Fecha de entrega: 12-03-2024

Observaciones: Excelente trabajo chicos.

CALIFICACIÓN: 10

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	77/479
		Sección ISO	8.3
		Fecha de emisión	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada.			

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	78/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno o la alumna al finalizar la práctica, se familiarizará con el manejo de algunas herramientas del Sistema Operativo Linux, como son route y traceroute, y sus similares en Windows, como son route y tracert, enfocadas al encaminamiento de paquetes a través de la red.
- El alumno o la alumna conocerá los fundamentos del monitoreo de redes.
- El alumno o la alumna aplicará filtros adecuados en el análisis de paquetes.
- El alumno o la alumna realfirmará los conocimientos teóricos acerca del protocolo ARP mediante observación de casos reales.

2.- Conceptos teóricos

Práctica 6

Route

Este comando se utiliza para configurar las tablas de encaminamiento del núcleo de nuestro sistema. Generalmente en todo equipo de una red local tenemos al menos tres rutas: la de loopback, utilizando el dispositivo de bucle interno (lo, lo0...), la de red local (localnet), que utiliza la tarjeta de red para comunicarse con equipos dentro del mismo segmento de red, y una default que también utiliza la tarjeta para enviar a un router o gateway paquetes que no son para equipos de nuestro segmento.

Si route nos muestra una configuración sospechosa (esto es, las tablas no son las que en el sistema hemos establecido como administradores, aunque todo funcione correctamente) esto puede denotar un ataque de simulación: alguien ha desviado el tráfico por un equipo que se comporta de la misma forma que se comportaría el original, pero que seguramente analiza toda la información que pasa por él. Hemos de recalcar que esto suele ser transparente al buen funcionamiento del equipo (no notamos ni pérdida de paquetes, ni retardos excesivos, ni nada sospechoso) y que además el atacante puede modificar los archivos de arranque del sistema para, en caso de reinicio de la máquina, volver a tener configuradas las rutas a su gusto; estos archivos suelen ser del tipo /etc/rc.d/rc.inet1 o /etc/rc?d/Sinet.

También es posible que alguien esté haciendo uso de algún elemento utilizado en la conexión entre nuestro sistema y otro (un router, una pasarela...) para amenazar la integridad de nuestro equipo; si queremos comprobar el camino que siguen los paquetes desde que salen de la máquina hasta que llegan al destino, podemos utilizar la orden traceroute. Sin embargo, este tipo de ataques es mucho más difícil de detectar, y casi la única herramienta factible para evitarlos es la criptografía.

Encaminamiento y análisis de paquetes

Capa 3 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	79/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Traceroute

La orden traceroute se utiliza para imprimir la ruta que los paquetes siguen desde nuestro sistema hasta otra máquina, realizar pruebas, medidas y administración de una red; introduce mucha sobrecarga, lo que evidentemente puede acarrear problemas de rendimiento, llegando incluso a negaciones de servicio por el elevado tiempo de respuesta que el resto de aplicaciones de red pueden presentar.

Traceroute es una herramienta que combina muy inteligentemente, dos características de los protocolos que hacen posible Internet. Éstos son:

a) TTL o expiración de los paquetes

Para proteger a Internet del efecto de paquetes atrapados en ciclos de encajamiento, los diseñadores de TCP/IP dotaron a cada datagrama IP de un contador que llamaron TTL, por las siglas de *Time To Live*. Esto es un número que limita cuántos saltos puede dar un datagrama, antes de ser descartado por la red.

Cuando se introduce un datagrama IP a la red, el campo TTL es poblado con el número máximo de saltos que define la vida de ese datagrama. Cada router por el que ese datagrama transita, resta uno a ese número. Cuando éste llega a cero, el datagrama es descartado.

b) Internet Control Message Protocol o ICMP

ICMP sirve para manejar mensajes de control. Esto son mensajes administrativos entre nodos de Internet. Los paquetes ICMP sirven para muchas cosas: avisar que un enlace o que un dispositivo están congestionados, que se escogió un camino sub-óptimo para enviar un paquete, que no se puede acceder a un sitio en particular, etcétera, uno de esos avisos es particularmente útil para traceroute: El aviso de que se excedió la vida útil del paquete.

Combinando estas dos herramientas, traceroute permite construir un mapa de la red tal como es vista desde un nodo en particular.

Aquí se muestra cada uno de los saltos que tiene que dar un paquete al recorrer el camino desde la computadora hasta www.unam.mx. La dirección del recorrido es muy importante, porque en Internet no necesariamente el camino de ida es igual al de regreso.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	80/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

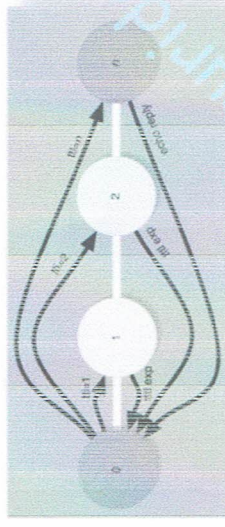


Figura No.1. Funcionamiento de Traceroute

El ejemplo anterior permite ver mejor cómo funciona la herramienta. (Ver Figura No. 1). En el primer salto, hacia el nodo 1, traceroute pone el valor TTL en 1 y envía el paquete hacia el nodo de destino. Cuando el nodo 1 decrementa el valor del TTL, obtiene un cero, devuelve al nodo de origen un mensaje de error que dice que el TTL expiró mientras el paquete iba en tránsito. Este proceso se repite varias veces y los tiempos se registran.

Para el siguiente salto, traceroute aumenta en uno el valor del TTL y lo envía de nuevo hacia su destino. El nodo 1 decrementa el valor del TTL a uno y pasa el paquete hacia el nodo 2. El nodo 2 recibe el paquete con TTL uno y al decrementarlo, obtiene un TTL cero, enviando el correspondiente mensaje de error hacia el nodo de origen. Este proceso se va repitiendo con valores progresivamente más grandes de TTL, para ir encontrando los saltos cada vez más lejanos o hasta que se llega a un TTL muy grande. Típicamente este valor máximo es 30, aunque puede ser de hasta 255.

Análisis de paquetes

El análisis de paquetes resulta una herramienta fundamental en dos sentidos. Por un lado, permite apreciar de forma realista muchos de los conceptos fundamentales de las redes en general, y de los protocolos TCP/IP en particular (encapsulación, fragmentación, secuenciación de mensajes, etc). Por otro lado, permite realizar un diagnóstico muy preciso de las redes en funcionamiento, desde la detección de errores, la verificación de los mecanismos de seguridad y la evaluación de prestaciones de la red.

Es por ello que en esta práctica se estudiará una herramienta gratuita de análisis de paquetes, denominada Wireshark, que trabaja sobre una interfaz de red denominada WinPcap.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	81/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

La captura de tramas consiste en la obtención directa de tramas tal y como aparecen a nivel de LAN. Puesto que el medio de transmisión es generalmente, una línea de difusión, el monitorio permite observar la totalidad de las comunicaciones que tienen lugar a través de la red, y por tanto resulta una herramienta muy potente, tanto desde el punto de vista positivo (diagnóstico de red) como el negativo (compromete la confidencialidad de las comunicaciones)

La cantidad de información obtenida de una captura de paquetes es enorme. Por tanto, es necesario establecer filtros de aceptación que permitan que las tramas no consideradas relevantes no se almacenen ni muestren al usuario.

El paquete Wireshark

Es una aplicación completamente configurable para el análisis mediante monitoreo de redes locales en entornos TCP/IP sobre cualquiera de las tecnologías soportadas por la interfaz WinPcap.

3.- Equipo y material necesario Equipo del laboratorio:

- Computadora con sistema operativo Linux Debian y Windows
- Herramienta Wireshark instalada en el sistema Windows

4.- Desarrollo:

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Encaminamiento y análisis de paquetes bajo plataforma Linux

4.1.1 Abre la aplicación VirtualBox

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectar a: Adaptador puente (Figura No. 2)


	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	82/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			




Figura No. 2. Conexión de red.

4.1.2 Encienda la máquina virtual

4.1.3 Elija la opción de cargar Linux, distribución Debian.

4.1.4 Inicie sesión como usuario redes. La profesora o el profesor le proporcionará la contraseña

4.1.5 Abra una terminal e ingrese como super usuario, teclee la contraseña de root. (Ver Figura No. 3)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	83/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			


	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	84/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



Figura No. 3. Terminal de comandos.

4.1.6 Verifique que la conexión a la red esté habilitada (Ver Figura No. 4).



Figura No. 4. Conexión a la red.

4.1.7 Monitoree la interfaz de red, para ello teclee el siguiente comando (Figura No. 5)

NOTA: Para realizar la práctica exitosamente debe tener instalado el paquete tcpdump.

root@debian:/home/redes# tcpdump -i enp0s3

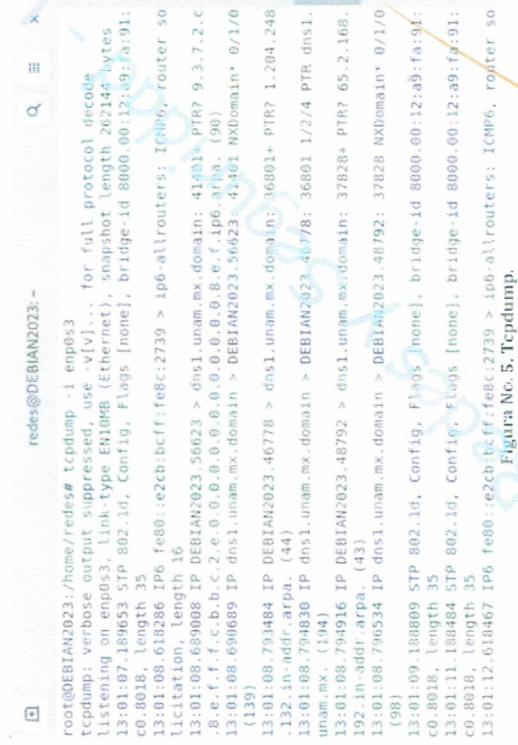



Figura No. 5. Tcpdump.

NOTA: Teclee ctrl+c para detener la captura

4.1.8 Analice la salida en pantalla y trate de identificar direcciones IP's, puertos, nombres, protocolos, etcétera y escríbalos a continuación:

Dirección	Puerto	Nombre	Protocolo
205.198-204-191	443	bestelclientes	UDP
204.198-204-191	443	bestelclientes	UDP

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	85/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.9 Visualice la configuración actual de la tabla de enrutamiento. (Ver Figura No. 6)
Teclee lo siguiente:

```
root@debian:/home/redes# route
```

```
root@debian:/home/redes# route
```

Kernel IP routing table	Destination	Gateway	Genmask	Flags	Metric	Use	Interface
default	0.0.0.0	0.0.0.0	0.0.0.0	U	0	0	eth0
192.168.2.0	192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	eth0

Figura No. 6. Comando route

4.1.10 Analice la tabla y explique cada una de sus partes; así como la importancia de la misma.

La columna de destination es la dirección a la que viaja el paquete, Gateway es por eso donde sale Genmask, es máscara de sub red, flags metric es la distancia a la dirección objetivo Ref son las referencias a la ruta, Use, son las conexiones realizadas a la ruta y finalmente Interface es la interfaz a la que serán enviados los paquetes

4.1.11 Observe la ruta que sigue un paquete por la red. Teclee lo siguiente: (Ver Figura No. 7)

```
root@debian:/home/redes# traceroute www.google.com
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	86/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		

La impresión de este documento es una copia no controlada

La impresión de este documento es una copia no controlada

```
root@DEBIAN2023:/home/redes# traceroute www.google.com
```

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1040	1041	1042	1043	1044	1045	1046	1047	1048	1049	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1060	1061	1062	1063	1064	1065	1066	1067	1068	1069	1070	1071	1072	1073	1074	1075	1076	1077	1078	1079	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089	1090	1091	1092	1093	1094	1095	1096	1097	1098	1099	1100	1101	1102	1103	1104	1105	1106	1107	1108	1109	1110	1111	1112	1113	1114	1115	1116	1117	1118	1119	1120	1121	1122	1123	1124	1125	1126	1127	1128	1129	1130	1131	1132	1133	1134	1135	1136	1137	1138	1139	1140	1141	1142	1143	1144	1145	1146	1147	1148	1149	1150	1151	1152	1153	1154	1155	1156	1157	1158	1159	1160	1161	1162	1163	1164	1165	1166	1167	1168	1169	1170	1171	1172	1173	1174	1175	1176	1177	1178	1179	1180	1181	1182	1183	1184	1185	1186	1187	1188	1189	1190	1191	1192	1193	1194	1195	1196	1197	1198	1199	1200	1201	1202	1203	1204	1205	1206	1207	1208	1209	1210	1211	1212	1213	1214	1215	1216	1217	1218	1219	1220	1221	1222	1223	1224	1225	1226	1227	1228	1229	1230	1231	1232	1233	1234	1235	1236	1237	1238	1239	1240	1241	1242	1243	1244	1245	1246	1247	1248	1249	1250	1251	1252	1253	1254	1255	1256	1257	1258	1259	1260	1261	1262	1263	1264	1265	1266	1267	1268	1269	1270	1271	1272	1273	1274	1275	1276	1277	1278	1279	1280	1281	1282	1283	1284	1285	1286	1287	1288	1289	1290	1291	1292	1293	1294	1295	1296	1297	1298	1299	1300	1301	1302	1303	1304	1305	1306	1307	1308	1309	1310	1311	1312	1313	1314	1315	1316	1317	1318	1319	1320	1321	1322	1323	1324	1325	1326	1327	1328	1329	1330	1331	1332	1333	1334	1335	1336	1337	1338	1339	1340	1341	1342	1343	1344	1345	1
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	---

	Manual de prácticas del Laboratorio de Redes de Datos Segura <i>s</i>	Código:	MADO-31
		Versión:	06
		Página	87/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

La tabla que nos dio windows es muy similar a la obtenida en linux pero tiene menos columnas, tiene Destination, Mask, Gateway, Interface y Metric. En windows a diferencia de linux, nos proporciona la IP. Podríamos ver las interfaces de nuestros equipos como virtual, indembri, etc.

4.2.6 Observe el camino que sigue un paquete. Teclee lo siguiente:

C:\> tracert www.google.com

4.2.7 Analice el resultado del paso anterior y comente:

Nos dio una traza completa con IPv6 con un formato distinto al de linux. Al activar de la tarjeta #5 volvió a retransmitir de acuerdo a que nos dio IPv6, si hubiera sido IPv4 nos hubiera salido como en linux.

4.2.8 Utilización de la aplicación Wireshark

4.2.8.1 Abra la aplicación de Wireshark

4.2.8.2 Dé clic en el menú Capture y elija Options.

4.2.8.3 Seleccione y habilite la tarjeta de red que está usando (Interface) dando doble clic sobre ella.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	88/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Fieides y Seguridad		
La impresión de este documento es una copia no controlada			

4.2.8.4 Deshabilite la opción Activar modo promiscuo en todas las interfaces. Oprima Iniciar (Ver Figura No. 8)

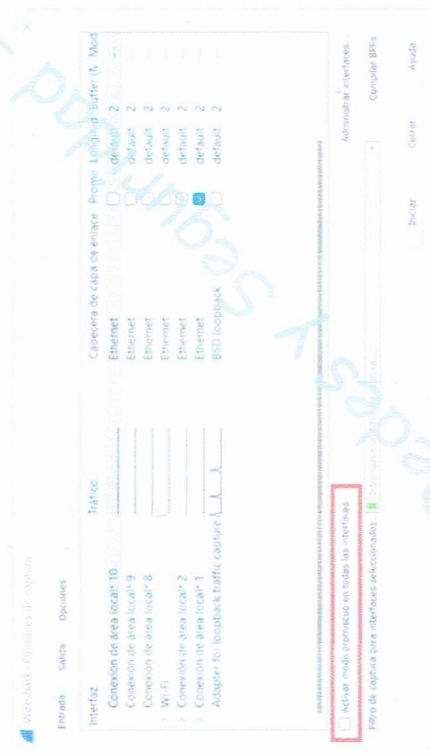



Figura No. 8. Opciones de captura.

4.2.8.5 Dé clic en la opción Analizar y seleccione del menú Mostrar expresión de filtro dar clic en la siguiente opción: ARP/RARP -> Address Resolution Protocol-> arp.protocol.type-> Protocol type. Dé clic en Aceptar (Ver Figura No. 9)

	Manual de prácticas del Laboratorio de Redes de Datos Segura	Código:	MADO-31
		Versión:	06
		Página	89/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	90/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Fieides y Seguridad		
La impresión de este documento es una copia no controlada			

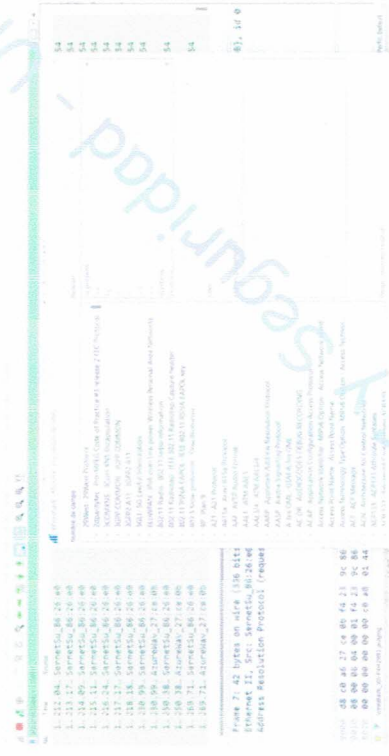


Figura No. 9. Filtro ARP.

4.2.8.6 Seleccione la flecha azul para aplicar el filtro seleccionado (Ver figura No. 10)

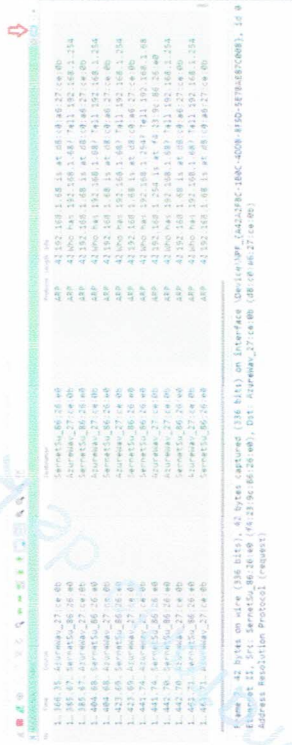


Figura No. 10. Aplicación del filtro ARP.

4.2.8.7 En la terminal de comandos ejecute el comando ping a 5 destinos diferentes, dos de ellos fuera de la red local y el resto a computadoras dentro de la red local.

4.2.8.8 Visualice la tabla de ARP, para ello teclee lo siguiente:

C:\> arp -a

4.2.8.9 Detenga la captura de Wireshark.

4.2.8.10 Realice una tabla con el contenido de la tabla del comando ARP del paso 4.2.8.7.

Interface	192.168.1.85
Direction	Internet
Direction física	38-p9-d3-3c-e2-a2
IP	192.168.3.74
MAC	755.255.255.255
MAC física	ff-ff-ff-ff-ff-ff
MAC física	estático

4.2.8.11 Analice la información del paso anterior y comente

Los muestre únicamente las direcciones en nuestra red local, si el muestreo el filtro nos aparece otros

4.2.8.12 Vuelva a Wireshark y observe las tramas recibidas

4.2.8.13 Localice una trama ARP REQUEST y su correspondiente ARP REPLY. Analice las características de ambas tramas (Direcciones físicas y lógicas, de origen y destino) y escriba a continuación lo que observa para reconocer una trama ARP REQUEST y una trama ARP REPLY, indique cuál es el funcionamiento del protocolo ARP (Figura No. 11):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras:			Código: Versión: Página Sección ISO	MADO-31 06 93/479 8 3
Facultad de Ingeniería		Fecha de emisión 11 de agosto de 2023			
		Área/Departamento: Laboratorio de Redes y Seguridad			
La impresión de este documento es una copia no controlada					

PRÁCTICA 6
Encaminamiento y análisis de paquetes
Questionario Previo

1. Describa las funciones de la capa 3 (capa de red) del Modelo OSI
2. ¿Cuáles son los principales campos que forman la trama Ethernet?
3. ¿Cuáles son los principales campos que forman un paquete IP?
4. ¿Para qué se usa el comando apt-get install tcpdump o apt install tcpdump?
5. Defina el concepto de encaminamiento
6. Investigue el objetivo y funcionamiento del protocolo ARP
7. Descargue el software NeoTrace (o equivalente) y visualice en el modo Node View el camino que siguen los paquetes hacia un servidor localizado en:
 - a. www.google.com
 - b. www.youtube.com
 - c. wikipedia.com
 - d. Otra liga de su preferencia
8. Realice impresiones de pantalla e inclúyalas en la entrega de este previo.
 Allí, emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.