

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

**Lab17 - Filter on Traffic to or from Online
Backup Subnets**

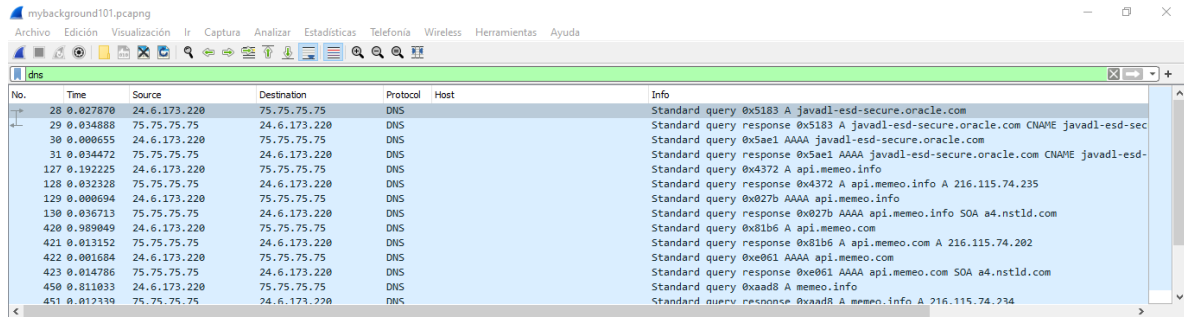
Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

Lab17 - Filter on Traffic to or from Online Backup Subnets

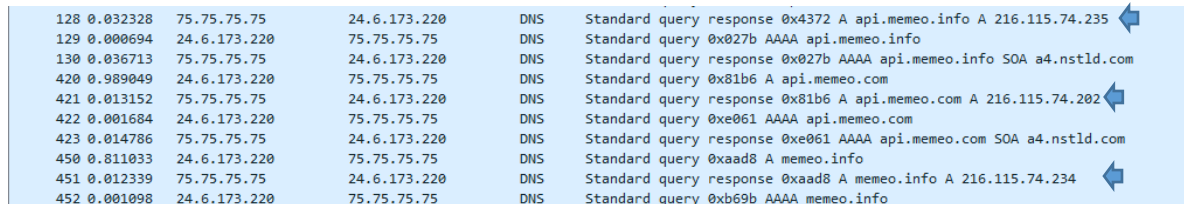
1 Abrimos el archivo mybackground101.pcapng

2 Aplicamos el filtro DNS



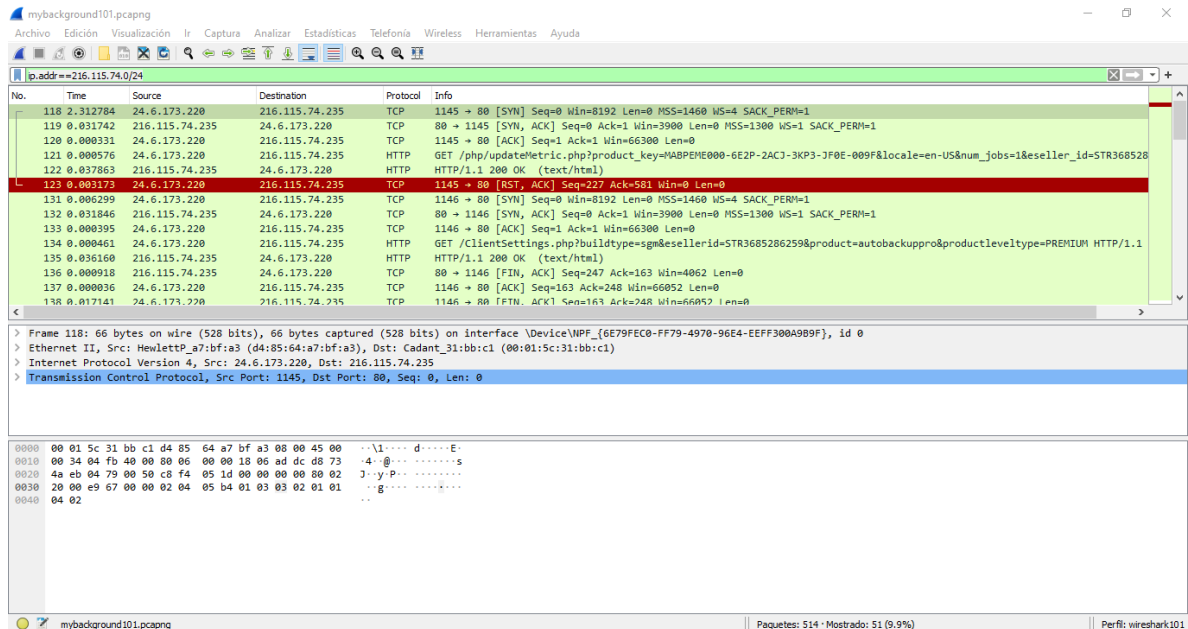
No.	Time	Source	Destination	Protocol	Host	Info
28	0.027870	24.6.173.220	75.75.75.75	DNS		Standard query 0x5183 A javadl-esd-secure.oracle.com
29	0.034888	75.75.75.75	24.6.173.220	DNS		Standard query response 0x5183 A javadl-esd-secure.oracle.com CNAME javadl-esd-sec
30	0.000655	24.6.173.220	75.75.75.75	DNS		Standard query 0x5ae1 AAAA javadl-esd-secure.oracle.com
31	0.034472	75.75.75.75	24.6.173.220	DNS		Standard query response 0x5ae1 AAAA javadl-esd-secure.oracle.com CNAME javadl-esd-
127	0.192225	24.6.173.220	75.75.75.75	DNS		Standard query 0x4372 A api.memeo.info
128	0.032328	75.75.75.75	24.6.173.220	DNS		Standard query response 0x4372 A api.memeo.info A 216.115.74.235
129	0.000694	24.6.173.220	75.75.75.75	DNS		Standard query 0x027b AAAA api.memeo.info
130	0.036713	75.75.75.75	24.6.173.220	DNS		Standard query response 0x027b AAAA api.memeo.info SOA a4.nstld.com
420	0.989049	24.6.173.220	75.75.75.75	DNS		Standard query 0x81b6 A api.memeo.com
421	0.013152	75.75.75.75	24.6.173.220	DNS		Standard query response 0x81b6 A api.memeo.com A 216.115.74.202
422	0.001684	24.6.173.220	75.75.75.75	DNS		Standard query 0xe061 AAAA api.memeo.com
423	0.014786	75.75.75.75	24.6.173.220	DNS		Standard query response 0xe061 AAAA api.memeo.com SOA a4.nstld.com
450	0.811893	24.6.173.220	75.75.75.75	DNS		Standard query 0xaad8 A memeo.info
451	0.012339	75.75.75.75	24.6.173.220	DNS		Standard query response 0xaad8 A memeo.info A 216.115.74.234

Podemos observar que api.memeo.info, api.memeo.com y memeo.info.host tiene una dirección ip de 216.115.74.



128	0.032328	75.75.75.75	24.6.173.220	DNS	Standard query response 0x4372 A api.memeo.info A 216.115.74.235
129	0.000694	24.6.173.220	75.75.75.75	DNS	Standard query 0x027b AAAA api.memeo.info
130	0.036713	75.75.75.75	24.6.173.220	DNS	Standard query response 0x027b AAAA api.memeo.info SOA a4.nstld.com
420	0.989049	24.6.173.220	75.75.75.75	DNS	Standard query 0x81b6 A api.memeo.com
421	0.013152	75.75.75.75	24.6.173.220	DNS	Standard query response 0x81b6 A api.memeo.com A 216.115.74.202
422	0.001684	24.6.173.220	75.75.75.75	DNS	Standard query 0xe061 AAAA api.memeo.com
423	0.014786	75.75.75.75	24.6.173.220	DNS	Standard query response 0xe061 AAAA api.memeo.com SOA a4.nstld.com
450	0.811893	24.6.173.220	75.75.75.75	DNS	Standard query 0xaad8 A memeo.info
451	0.012339	75.75.75.75	24.6.173.220	DNS	Standard query response 0xaad8 A memeo.info A 216.115.74.234
452	0.001098	24.6.173.220	75.75.75.75	DNS	Standard query 0xb69b AAAA memeo.info

3. Aplicamos el filtro ip.addr==216.115.74.0/24 para poder observar el tráfico.



No.	Time	Source	Destination	Protocol	Info
118	2.312784	24.6.173.220	216.115.74.235	TCP	1145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
119	0.031742	216.115.74.235	24.6.173.220	TCP	80 → 1145 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1300 WS=1 SACK_PERM=1
120	0.000331	24.6.173.220	216.115.74.235	TCP	1145 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
121	0.000576	24.6.173.220	216.115.74.235	HTTP	GET /php/updateMetric.php?product_key=NABPEHE000-6E2P-2ACJ-3KP3-JF0E-009F&locale=en-US&num_jobs=1&reseller_id=STR368528
122	0.037863	216.115.74.235	24.6.173.220	HTTP	HTTP/1.1 200 OK (text/html)
123	0.003173	24.6.173.220	216.115.74.235	TCP	1145 → 80 [RST, ACK] Seq=227 Ack=581 Win=0 Len=0
131	0.000299	24.6.173.220	216.115.74.235	TCP	1146 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
132	0.031846	216.115.74.235	24.6.173.220	TCP	80 → 1146 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1300 WS=1 SACK_PERM=1
133	0.000395	24.6.173.220	216.115.74.235	TCP	1146 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
134	0.000461	24.6.173.220	216.115.74.235	HTTP	GET /clientSettings.php?builtype=sgm&resellerid=STR3685286259&product=autobackuppro&productleveltype=PREMIUM HTTP/1.1
135	0.036160	216.115.74.235	24.6.173.220	HTTP	HTTP/1.1 200 OK (text/html)
136	0.000918	216.115.74.235	24.6.173.220	TCP	80 → 1146 [FIN, ACK] Seq=247 Ack=163 Win=4062 Len=0
137	0.000036	24.6.173.220	216.115.74.235	TCP	1146 → 80 [ACK] Seq=163 Ack=248 Win=66052 Len=0
138	0.017141	24.6.173.220	216.115.74.235	TCP	1146 → 80 [FIN, ACK] Seq=163 Ack=248 Win=66052 Len=0

> Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bfa3 (d4:85:64:a7:bfa3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 216.115.74.235
> Transmission Control Protocol, Src Port: 1145, Dst Port: 80, Seq: 0, Len: 0

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1....d....E-
0010 00 34 04 fb 40 00 06 00 00 18 06 ad dc d8 73 .4.@.....s
0020 4a eb 04 79 00 50 c8 f4 05 1d 00 00 00 80 02 J..y:P.....
0030 20 00 e9 67 00 02 04 05 b4 01 03 03 02 01 01 .g.....
0040 04 02 ..

Deberá de proyectar 51 paquetes

Paquetes: 514 · Mostrado: 51 (9.9%)