

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#17 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

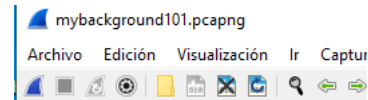
Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 3/Diciembre/2020

Horario: 5:00 pm – 6:00 pm

Laboratio N#17 – Filtrar el trafico hacia o desde subredes de respaldo en linea.

Paso 1 – Abrimos mybackground101.pcapng



Paso 2 – Aplicamos un filtro de visualización para el tráfico DNS hay que tener en cuenta las IP proporcionadas ya que todos comienzan con 216.115.74.

mybackground101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

dns

No.	Info	Source	Destination	Protocol
128	Standard query response 0x4372 A api.memeo.info A 216.115.74.235	75.75.75.75	24.6.173.220	DNS
29	Standard query response 0x5183 A javadl-esd-secure.oracle.com CNAME javadl-e...	75.75.75.75	24.6.173.220	DNS
31	Standard query response 0x5ae1 AAAA javadl-esd-secure.oracle.com CNAME javad...	75.75.75.75	24.6.173.220	DNS
421	Standard query response 0x81b6 A api.memeo.com A 216.115.74.202	75.75.75.75	24.6.173.220	DNS
451	Standard query response 0xaaad8 A memeo.info A 216.115.74.234	75.75.75.75	24.6.173.220	DNS
453	Standard query response 0xb69b AAAA memeo.info SOA a4.nstld.com	75.75.75.75	24.6.173.220	DNS
473	Standard query response 0xa0f1 AAAA api.memeo.com SOA a4.nstld.com	75.75.75.75	24.6.173.220	DNS

> Frame 28: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
> User Datagram Protocol, Src Port: 58537, Dst Port: 53
> Domain Name System (query)

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 01 00 00 00 00 00 11 00 00 18 06 ad dc 4b 4b
0010 4b 4b e4 a9 00 00 00 36 5c c0 51 83 01 00 00 01 KK 5 6 \ Q
0020 00 00 00 00 00 00 11 6a 61 76 61 64 6c 2d 65 73j avadl-es
0030 64 2d 73 65 63 75 72 65 06 6f 72 61 63 6c 65 03 d-secure -oracle-
0040 63 6f 6d 00 00 01 00 01 com.....

Domain Name System: Protocol Paquetes: 514 · Mostrado: 16 (3.1%) Perfil: wireshark101

Paso 3 – Aplicar un filtro de visualización para `ip.addr == 216.115.74.0 /24` y debe hacer 51 paquetes para que coincidan con su filtro de pantalla.

mybackground101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr==216.115.74.0/24

No.	Info	Source	Destination	Protocol
120	1145 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0	24.6.173.220	216.115.74.235	TCP
123	1145 → 80 [RST, ACK] Seq=227 Ack=581 Win=0 Len=0	24.6.173.220	216.115.74.235	TCP
118	1145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1	24.6.173.220	216.115.74.235	TCP
133	1146 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0	24.6.173.220	216.115.74.235	TCP
137	1146 → 80 [ACK] Seq=163 Ack=248 Win=66052 Len=0	24.6.173.220	216.115.74.235	TCP
138	1146 → 80 [FIN, ACK] Seq=163 Ack=248 Win=66052 Len=0	24.6.173.220	216.115.74.235	TCP
131	1146 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1	24.6.173.220	216.115.74.235	TCP

> Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFF300A9B9F}, id 0

> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), 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

mybackground101.pcapng Paquetes: 514 · Mostrado: 51 (9.9%) Perfil: wireshark101

Paso 4 – Hacemos clic en borrar para quitar el filtro de pantalla para continuar.

mybackground101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Info	Source	Destination	Protocol
-----	------	--------	-------------	----------