TP4- Análise de tráfego

Cibersegurança

João Pedro Ferreira Neto - pg50810@alunos.uminho.pt

João Pedro Sousa Moura - a93099@alunos.uminho.pt

José Pedro Fernandes Peleja - a84436 @alunos.uminho.pt

Rodrigo Almeida Bobzien - a84215@alunos.uminho.pt

Sandro Teixeira Ribeiro - a85316@alunos.uminho.pt

Índice

Índice de figuras

Índice de tabelas

1. Home net = 193.137.8.0/24

Após uma primeira análise do tráfego foi concluído que o tráfego foi muito provavelmente capturado através do IP 193.137.8.106. Este é o endpoint com maior número de pacotes a serem transmitidos/recebidos.

Como na lista de endpoints observamos mais IPs começados por 193.137.8.x, isto confirma que a rede local desta captura de tráfego se trata da rede 193.137.8.0/24.

2. Análise estatística e Caracterização geral

Para que fosse possível realizar uma análise e caracterização geral do tráfego foram utilizadas ferramentas disponíveis no Wireshark dentro do menu de *Statistics.* Dentro deste menu temos disponíveis as ferramentas EndPoints, I/O Graph e o capture File Properties para obter dados.

Com recurso da base de dados disponibilizada pela MaxMind e dentro da ferramenta EndPoints é possível verificar quem são os intervenientes nas comunicações e a localização aproximada dos mesmos. Na figura 1 é visível o mapa com as localizações dos IPs intervenientes nesta captura de tráfego.

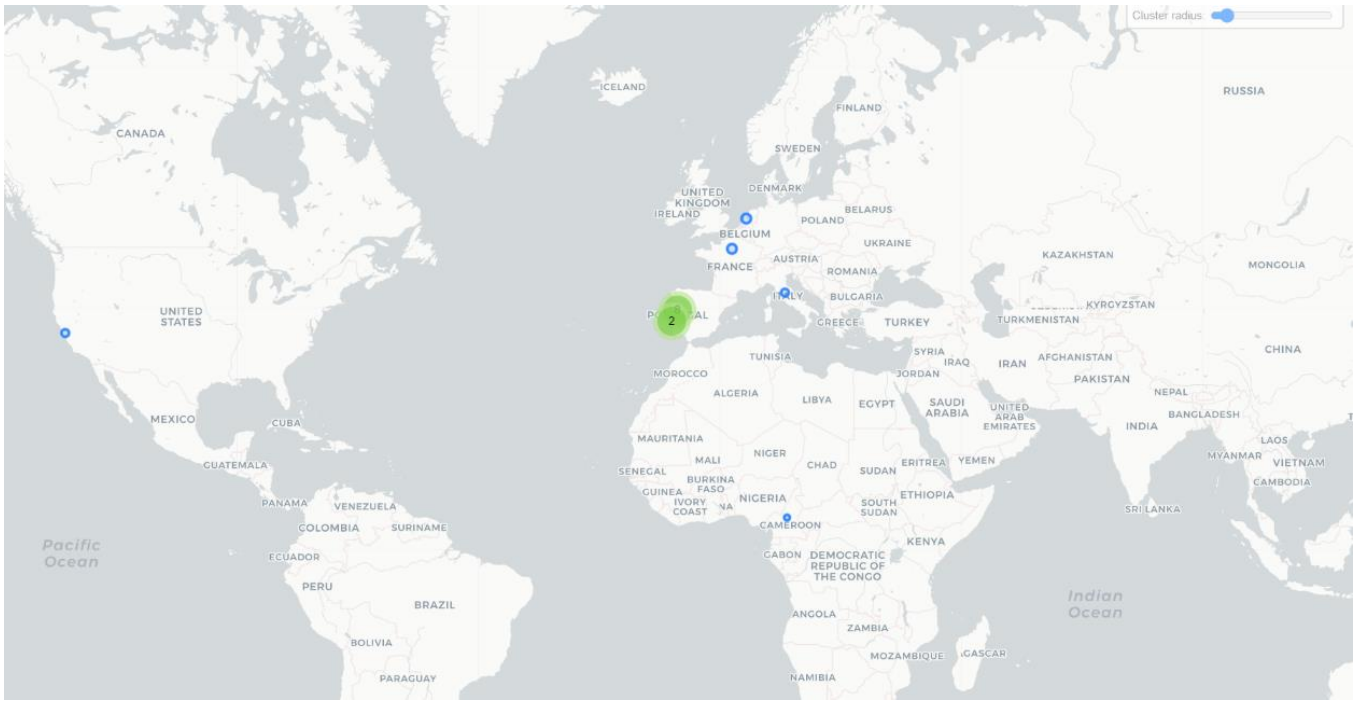


Figura 1- Mapa com as localizações dos IPs.

Na figura 2 é observável a divisão do tráfego que existe ao longo do tempo, sendo os pacotes TCP a maioria, representados a vermelho no gráfico. A verde estão presentes os pacotes UDP que são bastantes menos que os TCP e a cinza estão os pacotes ICMP. Por fim temos os residuais a amarelo que são pacotes ARP e LOOP.

O gráfico da figura 2 também ajuda a situar em contexto temporal onde ocorreram os vários tipos de protocolos.

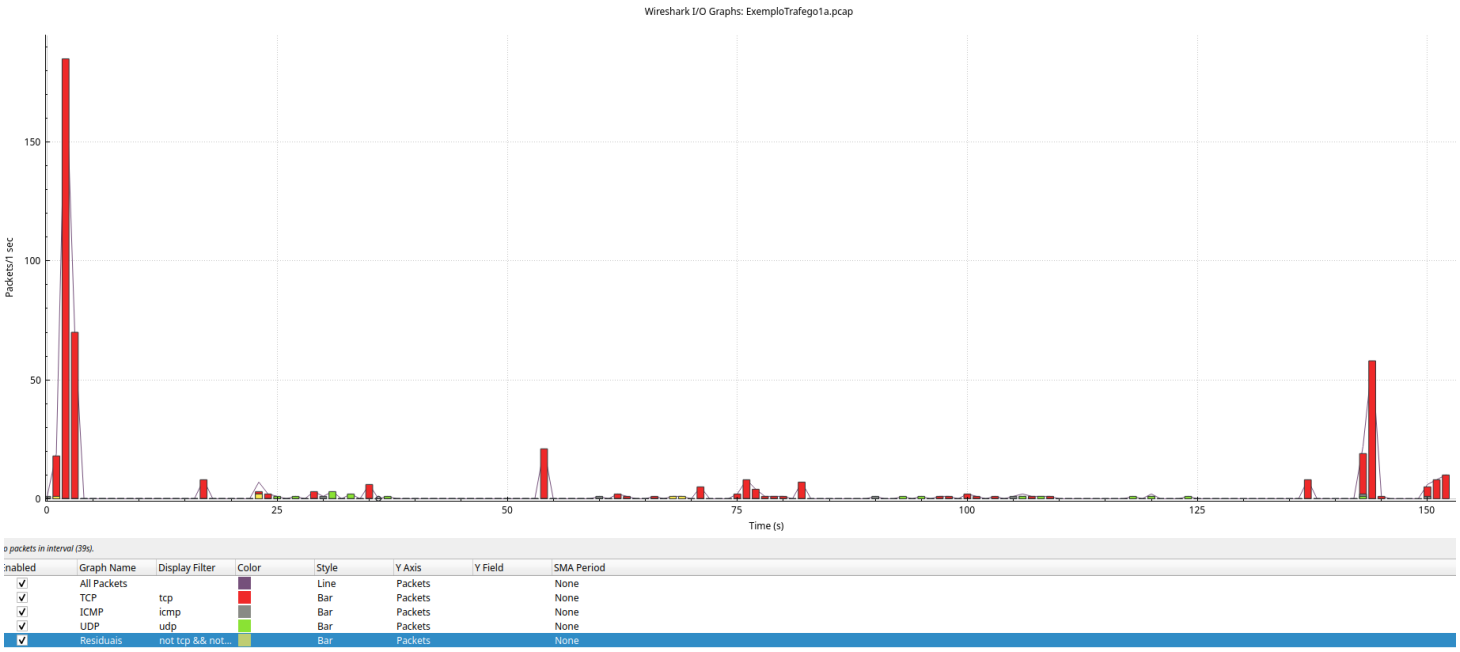


Figura 2- Gráfico da captura de tráfego.

De forma a obter informações aprofundadas sobre o tipo de pacotes foi usado o menu Protocol Hierarchy e obtivemos os resultados presentes na figura 3. Aqui podemos observar as percentagens referentes a cada protocolo, seja UDP ou TCP ou restantes, de salientar que 93.6% são pacotes TCP. Além dos valores percentuais conseguimos também retirar deduções extra sobre o tráfego como a quantidade de bytes assim como a sua percentagem, a taxa de transferência, entre outros.

Wireshark · Protocol Hierarchy Statistics · ExemploTrafego1a.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	499	100.0	173017	9057	0	0	0
Ethernet	100.0	499	4.0	6986	365	0	0	0
Internet Protocol Version 4	99.0	494	5.7	9880	517	0	0	0
User Datagram Protocol	3.6	18	0.1	144	7	0	0	0
NetBIOS Name Service	0.2	1	0.0	62	3	1	62	3
Domain Name System	0.4	2	0.1	90	4	2	90	4
Data	3.0	15	0.8	1361	71	15	1361	71
Transmission Control Protocol	93.6	467	88.6	153343	8027	281	69196	3622
Telnet	6.0	30	0.2	287	15	30	287	15
NetBIOS Session Service	14.8	74	4.7	8117	424	0	0	0
SMB (Server Message Block Protocol)	14.8	74	4.5	7821	409	74	7821	409
Malformed Packet	0.2	1	0.0	0	0	1	0	0
Hypertext Transfer Protocol	15.0	75	52.8	91424	4786	69	69570	3641
Line-based text data	0.8	4	10.0	17318	906	4	18327	959
Data	0.4	2	1.6	2844	148	2	3220	168
File Transfer Protocol (FTP)	1.0	5	0.1	136	7	5	0	0
Data	0.2	1	0.0	1	0	1	1	0
Internet Control Message Protocol	1.8	9	0.4	624	32	9	624	32
Configuration Test Protocol (loopback)	0.4	2	0.1	92	4	0	0	0
Data	0.4	2	0.0	80	4	2	80	4
Address Resolution Protocol	0.6	3	0.1	120	6	3	120	6

Figura 3- Percentagens de cada protocolo.

Depois de observar outra ferramenta como o Capture File Properties conseguimos obter o número total de pacotes, o tempo total neste tráfego, o débito médio, tamanho médio de pacote, etc. Estas informações gerais do tráfego são apresentadas nas figuras seguintes.

Time

First packet:	2022-10-12 17:36:28
Last packet:	2022-10-12 17:39:01
Elapsed:	00:02:32

Figura 4- Informação extra.

Statistics

Measurement	Captured	Displayed	Marked
Packets	499	499 (100.0%)	—
Time span, s	152.819	152.819	—
Average pps	3.3	3.3	—
Average packet size, B	347	347	—
Bytes	173017	173017 (100.0%)	0
Average bytes/s	1132	1132	—
Average bits/s	9057	9057	—

Figura 5- Informação extra.

Após a analise do tráfego e de analisar as estatísticas, o grupo encontrou na stream 18 do TCP uma tentativa de login e observou a password inserida, isto acontece devido ao facto do protocolo TELNET não implementar encriptação, tornando este propício a ataques.

Na figura 6 podemos observar a tentativa de login e comprovar que de facto está presente uma password e login, que por acaso nesta situação está errada, no entanto podemos considerar uma vulnerabilidade, pois um atacante que esteja a capturar o tráfego na rede pode ter acesso à mesma.

Figura 6- Tentativa de login.

3. Estratégia de análise

3.1 Descoberta de informação relativamente aos IPs

Inicialmente foi necessário descobrir os vários endereços IP que estão envolvidos na troca de pacotes a analisar e as suas respetivas informações. Para obter as informações sobre os vários IPs, como o país, a cidade e o numero do AS que foi acedida a base de dados disponibilizada pela MaxMind. Na figura 7 estão apresentados os resultados obtidos.

Ethernet · 14 | IPv4 · 17 | IPv6 | TCP · 28 | UDP · 12

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
41.244.211.188	3	450	3	450	0	0	Cameroon	—	37620	VIETTEL-CM-AS
rate-limited-proxy-66-249-91-17.google.com	17	5630	8	3676	9	1954	United States	Mountain View	15169	GOOGLE
81-64-154-175.rev.numericable.fr	3	405	3	405	0	0	France	Meudon	15557	Societe Francaise Du Radiotelephone - SFR SA
84.41.174.73	3	408	3	408	0	0	Netherlands	—	8608	Esprit Telecom B.V.
acb1-84-91-17-250.netvisao.pt	2	228	2	228	0	0	Portugal	Benedita	13156	Nowo Communications, S.A.
host-87-28-58-222.business.telecomitalia.it	9	558	9	558	0	0	Italy	—	3269	Telecom Italia
172.16.40.125	1	98	1	98	0	0	—	—	—	—
172.16.170.81	7	782	0	0	7	782	—	—	—	—
piano.dsi.uminho.pt	67	4157	29	1979	38	2178	Portugal	Viseu	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub106.scom3.uminho.pt	463	169 k	224	25 k	239	144 k	Portugal	Viseu	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub114.scom3.uminho.pt	2	252	0	0	2	252	Portugal	Viseu	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub138.scom3.uminho.pt	2	248	2	248	0	0	Portugal	Viseu	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub142.scom3.uminho.pt	106	18 k	50	10 k	56	7364	Portugal	Viseu	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub157.scom3.uminho.pt	22	2297	0	0	22	2297	Portugal	Viseu	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub215.scom3.uminho.pt	273	141 k	152	127 k	121	13 k	Portugal	Viseu	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub013.scom-glt.uminho.pt	6	684	6	684	0	0	Portugal	Guardizela	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
a217-70-68-212.cpe.netcabo.pt	2	252	2	252	0	0	Portugal	—	2860	Nos Comunicacoes, S.A.

Figura 7- Informação relativa aos IPs.

3.2 Estatísticas do tráfego

De seguida, é realizada a analise estatística relativamente ao trafego em que é utilizado o menu *Statistics* do *Wireshark*. Todos os passos até agora enunciados serão aprofundados nas seguintes secções.

3.3 Análise de pacotes

Após obtida a informação sobre os IPs o grupo analisou os pacotes. A análise foi iniciada com as streams TCP e foi realizada em conjunto pelo grupo inteiro. De seguida, foi necessário realizar a analise de pacotes UDP, ICMP e dos restantes (tráfego residual) e foi dividida pelos elementos do grupo. Para que a analise fosse bem sucedida foi necessário estudo do Wireshark de modo a sermos mais eficientes na realização da procura de streams.

Tanto nas streams UDP como nas TCP é possível filtrar para obter a conversação total entre 2 endpoints, ilustrado na figura 8.

Figura 8- Conversação entre 2 Endpoints.

Na figura acima é possível obter o conteúdo dos pacotes TCP trocados entre o host e o servidor (host a vermelho e servidor a azul).

4. Síntese da análise

4.1 Análise TCP

Tabela 1-Análise TCP.

Nº Ordem e Stream	Tempo	Origem e Destino	Comentário
Stream 0 Pacotes 3 a 15 e 184 a 205	Inicio: 1.457307s Fim: 2.899307s Duração: 1.442s	Origem- 193.167.8.106 – Porta 1137 Destino- 193.167.8.215 – Porta 106	É iniciada e efetuada uma conexão TCP entre os pacotes 3 e 5 (entre o elemento com o endereço 193.167.8.106 como cliente e o elemento com endereço 193.167.8.215 comoservidor). Após isto é realizado um pedido HTTP (versão 1.1) a partir do endereço 193.167.8.106 para o endereço 193.167.8.215 com o intuito de aceder à página "moodle.dsi.uminho.pt" (através de um browser mozilla a correr num ambiente windows NT 5.1). O pedido HTTP é dado como finalizado com o código 200, ou seja, foi realizado com sucesso e a conexão TCP é terminada entre os pacotes 202 e 205. É de apontar que durante esta conexão há vários pacotes TCP que excediam a quantidade de dados máxima, o que é evidenciado pela existência de vários pacotes TCP acompanhados pela descrição "[TCP segment of a reassembled PDU]", o que equivale ao "continuation" do TCP. São transferidos 35 pacotes com um tamanho total de 19000 bytes.
Stream 1 Pacotes 16 a 166	Inicio: 1.789632s Fim: 2.250532s Duração: 0.4609s	Origem- 193.137.8.106 – Porta 1138 Destino- 193.137.8.215 – Porta 80	É efetuada uma conexão TCP com sucesso e em seguida é realizado um pedido HTTP do tipo GET “/moodle/theme/standard/styles.php”. Este recurso php é transferido entre os pacotes 20 a 162, sendo que não existe qualquer tipo de código de finalização do pedido HTTP. A ligação TCP é encerrada entre os pacotes 163 a 166. O pacote 66 chegou com erros o que despoletou o envio de ACK’s e retransmissão do mesmo pacote depois do pacote com recurso ao fast retransmission. Podemos também verificar a existência de vários pacotes do tipo “continuation” apatir do pacote 72. Isto acontece, uma vez que tipicamente os pacotes não podem exceder os 1314 bytes. Isto indica que o que estava a ser transmitido tinha um tamanho superior a 1314 bytes. Cerca de 151 pacotes, com tamanho total de 109000 bytes.

Stream 2 Pacotes 167 a 178	Inicio: 2.298130s Fim: 2.755881s Duração:0.457751s	Origem- 193.137.8.106 – Porta 1139 Destino- 193.137.8.215 – Porta 80	É íniciada uma conexão TCP entre o pacote 167 e 169 através de um threeway handshake. É então iniciado um pedido HTTP (1.1) GET "/moodle/theme/standardwhite/styles.php. O pedido HTTP finaliza corretamente, evidênciado pelo pacote 173 o qual indica que o pedido GET de conteúdo de texto/css foi finalizado com o código 200 (sucesso). A conexão TCP é encerrada corretamente entre os pacotes 174-178. São transferidos 35 pacotes com um tamanho total de 18814 bytes. São trocados 12 pacotes com um tamanho total de 2282 bytes.
Stream 3 Pacotes 179 a 216	Inicio: 2.756597s Fim: 3.180185s Duração:0.423588s	Origem- 193.137.8.106 – Porta 1140 Destino- 193.137.8.215 – Porta 80	É íniciada uma conexão TCP entre o pacote 179 e 181 através de um threeway handshake. É então iniciado um pedido HTTP (1.1) GET "/moodle/theme/standardlogo/styles.php. O pedido HTTP finaliza corretamente, evidenciado pelo pacote 207 o qual indica que o pedido GET de conteúdo de texto/css foi finalizado com o código 200 (sucesso). A conexão TCP é corretamente encerrada entre os pacotes 208 e 212. Contudo o ACK contido no pacote 212 é repetido duas vezes (pacote 213-214), o que leva a que sejam enviados dois pacotes RST (215-216), indicando um fim imediato (ou não gracioso) da ligação. São transferidos 16 pacotes com um tamanho total de 2125 bytes.
Stream 4 Pacotes 217 a 226	Inicio: 3.186662s Fim: 3.214152s Duração: 0.02749s	Origem- 193.137.8.106 – Porta 1141 Destino- 193.137.8.215 – Porta 80	É iniciada uma conexão TCP entre o pacote 217 e 219 através de um threeway handshake. É então iniciado um pedido HTTP (1.1) GET "/moodle/lib/javascript-static.js. O pedido HTTP é finalizado com o código 304 no pacote 222, o qual indica que o cliente já possui o recurso que pediu na sua memória cache e que este não foi modificado desde a última vez que o mesmo foi pedido pelo que não é necessário o transferir. A conexão TCP é corretamente encerrada entre os pacotes 223 e 226. São transferidos 10 pacotes com um tamanho total de 1376 bytes.

Stream 5 Pacotes 227 a 238	Inicio: 3.222860s Fim: 3.531489s Duração:0.308629s	Origem- 193.137.8.106 – Porta 1142 Destino- 193.137.8.215 – Porta 80	É iniciada uma conexão TCP entre o pacote 227 e 229 através de um threeway handshake. É então iniciado um pedido HTTP (1.1) GET "/moodle/lib/javascript-mod.php. O pedido HTTP é finalizado com o código 304 no pacote 232, o qual indica que o cliente já possui o recurso que pediu na sua memória cache e que este não foi modificado desde a última vez que o mesmo foi pedido pelo que não é necessário o transferir. A conexão TCP é encerrada entre os pacotes 237 e 238, contudo falta um ACK que confirma a finalização da conexão do cliente com o servidor. São transferidos 9 pacotes com um tamanho total de 1468 bytes.
Stream 6 Pacotes 234 a 245	Inicio: 3.516297s Fim: 3.544832s Duração:0.028535s	Origem- 193.137.8.106 – Porta 1143 Destino- 193.137.8.215 – Porta 80	É iniciada uma conexão TCP entre o pacote 234 e 236 através de um threeway handshake. É então iniciado um pedido HTTP (1.1) GET "/moodle/lib/overlib.js. O pedido HTTP é finalizado com o código 304 no pacote 241, o qual indica que o cliente já possui o recurso que pediu na sua memória cache e que este não foi modificado desde a última vez que o mesmo foi pedido pelo que não é necessário o transferir. A conexão TCP é corretamente encerrada entre os pacotes 242 e 245. São transferidos 10 pacotes com um tamanho total de 1366 bytes.
Stream 7 Pacotes 246 a 255	Inicio: 3.582964 s Fim: 3.613962s Duração:0.030998s	Origem- 193.137.8.106 – Porta 1144 Destino- 193.137.8.215 – Porta 80	É iniciada uma conexão TCP entre o pacote 246 e 248 através de um threeway handshake. É então iniciado um pedido HTTP (1.1) GET "/moodle/lib/cookies.js. O pedido HTTP é finalizado com o código 304 no pacote 251, o qual indica que o cliente já possui o recurso que pediu na sua memória cache e que este não foi modificado desde a última vez que o mesmo foi pedido pelo que não é necessário o transferir. A conexão TCP é corretamente encerrada entre os pacotes 252 e 255. São transferidos 10 pacotes com um tamanho total de 1364 bytes.

Stream 8 Pacotes 256 a 265	Inicio: 3.617197s Fim: 3.648826s Duração:0.031629s	Origem- 193.137.8.106 – Porta 1145 Destino- 193.137.8.215 – Porta 80	É íniciada uma conexão TCP entre o pacote 256 e 258 através de um threeway handshake. É então iniciado um pedido HTTP (1.1) GET "/moodle/lib/ufo.js. O pedido HTTP é finalizado com o código 304 no pacote 261, o qual indica que o cliente já possui o recurso que pediu na sua memória cache e que este não foi modificado desde a última vez que o mesmo foi pedido pelo que não é necessário o transferir.A conexão TCP é corretamente encerrada entre os pacotes 262 e 265.São transferidos 10 pacotes com um tamanho total de 1362 bytes.
Stream 9 Pacotes 266 a 275	Inicio: 3.663604s Fim: 3.713998s Duração:0.050394s	Origem- 193.137.8.106 – Porta 1146 Destino- 193.137.8.215 – Porta 80	É íniciada uma conexão TCP entre o pacote 266 e 268 através de um threeway handshake. É então iniciado um pedido HTTP (1.1) GET "/moodle/theme/standardlogo/logo.gif. O pedido HTTP é finalizado com o código 304 no pacote 271, o qual indica que o cliente já possui o recurso que pediu na sua memória cache e que este não foi modificado desde a última vez que o mesmo foi pedido pelo que não é necessário o transferir. A conexão TCP é corretamente encerrada entre os pacotes 272 e 275. São transferidos 10 pacotes com um tamanho total de 1395 bytes.

Stream 10 Pacotes 276 a 283 e 361	Inicio: 17.040244s Fim: 82.494246s Duração:65.454002s	Origem- 193.137.8.106 – Porta 1153 Destino- 66.249.91.17 – Porta 80	É iniciada uma conexão TCP entre o pacote 276 e 278 através de um threeway handshake. Após isto é iniciado um pedido HTTP (1.1) GET "/mail?/?ui=pb&tlt=115a67ba1f3". Como este tráfego não possui qualquer tipo de segurança que oculte a informação que passa por ele, ao analisar o pacote é possível perceber que o serviço que está a ser usado é o gmail-chat e que o e-mail usado para o envio do pedido é "someone@gmail.com". Analisando o pacote 281 também é possível ler o emissor e o assunto de várias mensagens/e-mails , por exemplo "program@mentornet.net MentorNet¢[MentorNet DS]: InterviewsªeFor Match with Sam Bartels) Henrique, Giving a good interview is a skill that we often learn …". Como a ligação TCP não é corretamente encerrada, provavelmente por ultrapassagem do timer para o envio de uma nova mensagem, visto que o tempo passado entre o pacote 283 e 361 é de 64.997978 segundos, a ligação é encerrada através de um pacote RST.São transferidos 9 pacotes com um tamanho total de 2775 bytes.
Stream 11 Pacotes 288 a 292, 295 a 297, 304 a 309	Inicio: 23.819398s Fim: 35.186792s Duração:11.367394s	Origem- 193.137.8.106 – Porta 1151 Destino- 193.137.8.95 – Porta 21	A conexão e estabelecida com 3 mensagens de handshake, em seguida e pedida a conexão ao servidor "piano.dsi.uminho.pt". O servidor responde com o código 220 mostrando-se disponível, o cliente faz um pedido de login com o utilizador antonious, o servidor responde como desconhecendo o user e encerra a comunicação. Pode-se concluir que o servidor está protegido contra tentativas de adivinhar as credenciais originais. São trocados 14 pacotes com um total de 918 bytes.

Stream 12 Pacotes 311 a 367	Inicio: 54.257406s Fim: 82.845997s Duração:28.588591s	Origem- 193.137.8.106 – Porta 1156 Destino- 193.137.8.215 – Porta 23	É iniciada uma ligação TCP entre o pacote 311 e 313 através de um threeway handshake, como esta ligação está a ser realizada na porta 23, podemos dizer que se trata de uma ligação telnet. O protocolo Telnet trata-se de um protocolo que permite a conexão entre um cliente e um servidor telnet, sendo que a partir do momento em que a ligação é estabelecida, estes podem trocar mensagens de controlo e as respostas a este comando, podendo o cliente realizar comandos sobre o lado do servidor como se estivesse a usar um terminal no mesmo. No pacote 334 é enviado um pacote "TCP Keep-Alive" de modo a manter a conexão ativa. Com a análise dos pacotes TELNET, é possível ver, dada a falta de segurança sobre o tráfego em questão, que a partir do pacote 330 o server-side começa o processo de autenticação do user, sendo que este tenta fazer login com o user guest e que a password, a qual é transmitida byte a byte como uma tentativa de aumentar a segurança, também é guest. Esta tentativa de login acaba por ser rejeitado visto que no pacote 359 o server-side diz que o login está incorreto, exigindo novamente a autenticação do cliente. Nos pacotes 362 e 363 a comunicação telnet termina, sendo a ligação, ligação tcp sobre a qual esta estava a funcionar terminada graciosamente entre os pacotes 364 e 367. São trocados 53 pacotes com um total de 3163 bytes.
Stream 13 Pacotes 371, 373, 378	Inicio: 98.607890s Fim: 107,601622s Duração: 8,9937s	Origem- 87.28.58.222 – Porta 1139 Destino- 193.137.8.157 – Porta 445	Tentativa da criação de uma ligação TCP a partir de um dispositivo da empresa telecomitalia, evidenciado pelo envio do pacote [SYN] para o servidor TCP presente na máquina com o endereço 193.137.8.157. Como este não obteve resposta, este retransmite este pedido 2 vezes, acabando por desistir. São trocados 3 pacotes com um total de 168 bytes.

Stream 14 Pacotes 372, 375, 380	Inicio: 98.607890s Fim: 107,601622s Duração: 8,9937s	Origem- 87.28.58.222 – Porta 1139 Destino- 193.137.8.157 – Porta 445	Tentativa da criação de uma ligação TCP a partir de um dispositivo da empresa telecomitalia, evidenciado pelo envio do pacote [SYN] para o servidor TCP presente na máquina com o endereço 193.137.8.157. Como este não obteve resposta, este retransmite este pedido 2 vezes, acabando por desistir. São trocados 3 pacotes com um total de 168 bytes.
Stream 15 Pacotes 374, 376, 382	Inicio: 100.221796s Fim: 109,203745s Duração: 8,9819s	Origem- 87.28.58.222 – Porta 1141 Destino- 193.137.8.157 – Porta 80	Tentativa da criação de uma ligação TCP a partir de um dispositivo da empresa telecomitalia, evidenciado pelo envio do pacote [SYN] para o servidor TCP presente na máquina com o endereço 193.137.8.157. Como este não obteve resposta, este retransmite este pedido 2 vezes, acabando por desistir. Como as 2 ligações anteriores também falharam na criação de uma ligação TCP, podemos assumir que existe algum problema no lado do servidor, visto que esta reserva o port do pedido, já que os pacotes que seguem o pacote [SYN], podendo indicar que o port da ligação está a ser reutilizado, indicando a possibilidade da existência problemas de inatividade no servidor. São trocados 3 pacotes com um total de 168 bytes.
Stream 16	Inicio: 3.222860s Fim: 3.531489s Duração: 0.308629s	Origem- 193.137.8.106 – Porta 1142 Destino- 193.137.8.215 – Porta 80	Tráfego para um serviço de email da google (gmail) porta http(80). A intenção deste trafego é enviar um email para "someone@gmail.com" como podemos ver no GET (pacote 390 onde é iniciada sessão no gmail) e estabelecida uma conexão com o servidor da google com 3 pacotes o primeiro syn para o servidor este por sua vez responde com um syn ack ao que o host responde com um ack. depois deste handshake aparece um pedido http do tipo GET a "/mail/?ui=pbtlt=115a67ba1f3" é recebida uma resresposta do tipo HTTP 200 Nesta conexão são enviados 8 pacotes com um total de 5630 bytes.

Stream 17 Pacotes 397, 399, 401, 402, 404, 406 a 475, 477 a 499	Inicio: 143.664551s Fim: 152.818884s Duração: 9,154333s	Origem- 193.137.8.106 – Porta 1158 Destino- 193.137.8.142 – Porta 445	Sessão SMB que é um protocolo de troca de ficheiros do windows. Como está a ser executado dentro da mesma rede, à partida não existem problemas do pacote 409 a 411. Podemos ver que alguém tenta aceder como root a pasta \\TROMXONE\IPC$ mas foi recusada. Outra tentativa de acesso também negada aconteceu nos pacotes 416 a 421 em que o user COTASMRS\testeos tenta aceder ao ficheiro AutoRun.info na pasta \\TROMXONE\SOFT. A mensagem de erro que esta tentativa obteve foi STATUS_OBJECT_NAME_NOT_FOUND. Ao longo da sessão também podemos observar que ocorreram perdas de pacotes e houve as respetivas retransmissões. São trocados 98 pacotes com um total de 17132 bytes.
Stream 18 Pacotes 400, 403, 405	Inicio: 143.676901s Fim: 143.720977s Duração: 0.044076s	Origem- 193.137.8.106 – Porta 1159 Destino-193.137.8.142 – Porta 139	Esta stream é constituída por 3 pacotes, um SYN respondido com um SYN ACK, que por sua vez é respondido com um RST encerrando assim a conexão. A quantidade de bytes transmitida é de 178.

4.2 Análise UDP

Em relação ao tráfego UDP, este é um número reduzido de pacotes em relação ao TCP foi de analise mais rápida. Os resultados estão representados na seguinte tabela.

Tabela 2- Análise UDP.

Nº Ordem e Stream	Tempo	Origem e Destino	Comentário
Stream 0 Pacotes 284, 286	Inicio: 23.779650s Fim: 23.79205s Duração: 0.0124s	Origem- 193.137.8.106 (endpub106.scom3.uminho.pt) – Porta 1030 Destino- 193.137.8.142 (endpub142.scom3.uminho.pt) – Porta 53	É realizado um pedido DNS pelo host (193.137.8.106) ao servidor (193.137.8.142). Este devolve o IP correspondente ao main name piano.dsi.uminho.pt. Este tem o IP 193.137.8.95. Foram transmitidos 2 pacotes com total de 174 bytes.
Stream 1 Pacotes 293, 294, 301	Inicio: 25.535682s Fim: 31.551482 Duração: 6.0158s	Origem- 41.244.211.188 – Porta 35953 Destino- 193.137.8.157 (endpub157.scom3.uminho.pt) - Porta 30797	Aqui são apenas trocados 3 pacotes com um total de 450 bytes. Através da sua análise não foi possível chegar a qualquer conclusão.
Stream 2 Pacotes 299,302, 310	Inicio: 31.271661s Fim: 37.313241s Duração: 6.04158s	Origem- 84.41.174.73 - Porta 38337 Destino- 193.137.8.157 (endpub157.scom3.uminho.pt) – Porta 30797	Aqui são apenas trocados 3 pacotes com um total de 408 bytes. Através da sua análise não foi possível chegar a qualquer conclusão.
Stream 3 Pacotes 300, 303	Inicio: 31.279818s Fim: 33.316818s Duração: 2.0370s	Origem- 217.70.68.212 (a217-70-68-212.cpe.netcabo.pt) – Porta 59342 Destino- 193.137.8.114 (endpub114.scom3.uminho.pt) - Porta 23897	Aqui são apenas trocados 2 pacotes com um total de 252 bytes. Através da sua análise não foi possível chegar a qualquer conclusão.
Stream 4 Pacotes 369, 370	Inicio: 93.723027s Fim: 95.745327s Duração: 2.0223s	Origem- 193.137.8.138 (endpub138.scom3.uminho.pt) – Porta 39284 Destino- 193.137.8.157 (endpub157.scom3.uminho.pt) – Porta 30797	Aqui são apenas trocados 2 pacotes com um total de 248 bytes. Através da sua análise não foi possível chegar a qualquer conclusão.
Stream 5 Pacotes 379, 381	Inicio: 106.453435s Fim: 108.509335s Duração: 2.0559s	Origem- 84.91.17.250 (acb1-84-91-17.netvisao.pt) – Porta 54035 Destino- 193.137.8.157 (endpub157.scom3.uminho.pt’ – Porta 30797	Aqui são apenas trocados 2 pacotes com um total de 228 bytes. Através da sua análise não foi possível chegar a qualquer conclusão.

Stream 6 Pacotes 383, 385,386	Inicio: 118.301230s Fim: 124.32783s Duração: 6.0266s	Origem- 81.64.154.175 (81-64-154-175.rev.numericable.fr) – Porta 43622 Destino- 193.137.8.157 (endpub157.scom3.uminho.pt) – Porta 30797	Aqui são apenas trocados 3 pacotes com um total de 405 bytes. Através da sua análise não foi possível chegar a qualquer conclusão.
Stream 7 Pacotes 398	Inicio: 143.672084s Fim: 143.672084s Duração: 0.0000s	Origem- 193.137.8.142 (endpub142.scom3.uminho.pt) – Porta 137 Destino- 193.137.8.106 (endpub106.scom3.uminho.pt) –Porta 137	Nesta análise foi possível observar um pedido NBNS (NetBIOS Name Service) vindo do host (193.137.8.142) ao servidor (193.137.8.106) através do pacote 398. Este serve para traduzir, tal como o DNS, um URL no seu respetivo endereço. Neste caso foi transmitido 1 pacote com 104 bytes.

4.3 Análise ICMP

Após realizar a análise da TDP e UDP realizamos a análise da captura de tráfego de ICMP. Este protocolo é utilizado para comunicar informações da camada de rede.

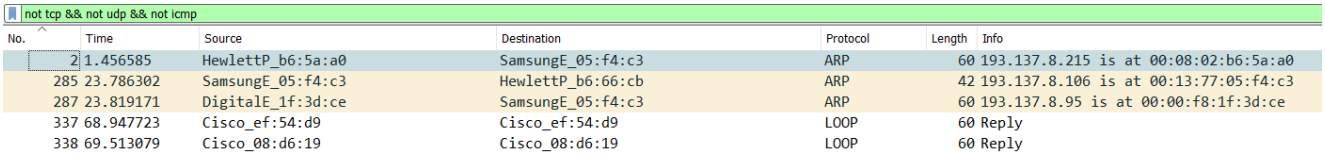
Tabela 3- Análise ICMP.

Nº de pacotes	Tempo	Origem e Destino	Comentário
Pacotes: 1, 298, 332, 368, 384, 476	Inicio: 0s Fim: 150.336312s Duração:150.336312s	Origem- 193.137.88.13 Destino- 172.16.170.81	É feito um *ping request* de 30 em 30 segundos, não sendo obtida resposta.
Pacotes: 377	Inicio: 105.037733s Fim: 105.037733s Duração: 0s	Origem- 172.16.40.125 Destino- 172.16.170.81	É feito um único ping request, não sendo obtida resposta.
Pacotes: 395, 396	Inicio: 143.654404s Fim:143.660955s Duração:0.006551s	Origem- 193.137.8.106 Destino- 193.137.8.142	É feito um *ping request* e é obtida resposta *ping reply,* ou seja, é realizado com sucesso do 193.137.8.106 para o 193.137.8.142.

4.4 Análise tráfego residual

Após analisar todo o trafego TCP, UDP e ICMP utilizamos o filtro “not tcp && not udp && not icmp” para podermos filtrar os restantes pacotes. Nesta captura de trafego obtivemos e observamos o protocolo ARP (usado na conversão de endereços de IP em endereços MAC da camada 2). Isto é demonstrado nas figuras 9 na secção de “Info”.

Em relação ao tráfego sob o protocolo LOOP é possível observar as portas que estão a receber e enviar tráfego, sendo que este protocolo, tal como o nome indica, é responsável por encontrar *loops* inesperados na rede, com a receção de tráfego na mesma porta em que o mesmo tráfego foi enviado.



not tcp && not udp && not icmp

No.	Time	Source	Destination	Protocol	Length	Info
2	1.456585	HewlettP_b6:5a:a0	SamsungE_05:f4:c3	ARP	60	193.137.8.215 is at 00:08:02:b6:5a:a0
285	23.786302	SamsungE_05:f4:c3	HewlettP_b6:66:cb	ARP	42	193.137.8.106 is at 00:13:77:05:f4:c3
287	23.819171	DigitalE_1f:3d:ce	SamsungE_05:f4:c3	ARP	60	193.137.8.95 is at 00:00:f8:1f:3d:ce
337	68.947723	Cisco_ef:54:d9	Cisco_ef:54:d9	LOOP	60	Reply
338	69.513079	Cisco_08:d6:19	Cisco_08:d6:19	LOOP	60	Reply

Figura 9- Tráfego residual.