UC/Curso: SRC/MIETI
Grupo 9:
Cláudia Cristiana de Amorim Dias 78232
David José Ressurreição Alves 79625

Trabalho Prático 4; ExemploTrafego1.pcap

1. Home net = 193.137.8.0/24

2. Estratégia de análise

1. Obter informações à cerca de todos os endereços IP's usados na captura presente no ficheiro (através da opção *Statistics→ Endpoints*), e de seguida usando a plataforma "www.whois.com", obter informações sobre os respetivos IP's.

2. Acrescentámos aos campos da tabela do wireshark o número de *stream* (através da opção *Column Preferences*)

3. Analisámos cada *stream* e os seus respetivos pacotes:

1º- Analisámos as *streams* TCP(através do filtro do wireshark tcp.stream);

2º- Estudamos os pacotes presentes em cada *stream* TCP (com o recurso à ferramenta do Wireshark "*Follow TCP Stream*");

3º- Analisámos as *streams* UDP(através do filtro do Wireshark udp.stream);

4º- Estudamos os pacotes presentes em cada *stream* UDP(com recurso à ferramenta do Wireshark "*Follow UDP Stream*")

4. Analisámos os restantes pacotes (que não pertenciam aos protocolos UDP nem TCP).

5. Obter informações à cerca da captura de dados presente no ficheiro (através da opção S*tatistics→Capture File Properties*);

6. Recorrendo a ferramentas de estatísticas do Wireshark, visualizamos estatísticas sobre a captura de rede analisada.

3. Síntese da análise

Para melhor compreensão da análise das capturas de tráfego TCP existe um anexo de figuras, neste documento.

TCP

Nº ordem ou *streams*	**Tempo (s)**	**Src/Dest**	**Comentário**
Stream: 0 **Pacotes:** 3 - 15 184 - 205	1.457307 a 2.899311 **Duração:** 1.442004	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1137 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	Do pacote 3 ao 5 é estabelecida uma conexão TCP recorrendo ao processo 3-way *Handshake* sendo posteriormente criada uma sessão HTTP. No pacote 6 é efetuado um pedido HTTP ao servidor para aceder à página "moodle.dsi.uminho.pt" sendo confirmada a receção de informação através de ACK's e dado termino à sessão (do pacote 202 a 205). Da *stream* 1 a 15 são enviados do servidor para o cliente elementos da página requerida nesta sessão de modo a ser possível a visualização da mesma. O número de total de pacotes transmitidos foi de 35 pacotes, num total de 19 kbytes.
Stream: 1 **Pacotes:** 16 - 166	1.789632 a 2.250563 **Duração:** 0.460931	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1138 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É estabelecida uma conexão TCP, sendo realizado um pedido HTTP GET de "/moodle/theme/standard/styles.php". Ocorreram falhas na receção de dados, concretamente no pacote 66 o que levou a envios de ACK's duplicados de modo a despoletar retransmissão do pacote em falta. Observa-se também que quando uma resposta apresenta um tamanho superior a 1314 bytes esta é repartida em vários pacotes (tamanho máximo de 1314 bytes), sendo apresentado a informação "*Continuation*" de modo a ser possível reconhecer essa situação. Uma vez que existe a receção de toda a informação, a conexão é fechada. O número de total de pacotes transmitidos foi de 151 pacotes, num total de 109 kbytes.
Stream: 2 **Pacotes:** 167 - 178	2.298130 a 2.755881 **Duração:** 0.457751	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1139 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	Nesta *stream* é estabelecida uma conexão TCP e posterior sessão HTTP, sendo realizado um pedido HTTP GET ao servidor de "/moodle/theme/standardwhite/styles.php" de modo a obter um ficheiro CSS, não havendo a ocorrência de erros. O número de total de pacotes transmitidos foi de 12 pacotes, num total de 2337 bytes.
Stream: 3 **Pacotes:** 179 - 183; 206 - 216	2.756597 a 3.180185 **Duração:** 0.423588	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1140 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É estabelecida uma conexão TCP, sendo efetuado um pedido HTTP GET, ao servidor, de "/moodle/theme/standardlogo/styles.php". Observa-se, depois de transferida a informação e terminada a conexão, que foram enviados ACK's duplicados provocando o envio de pacotes com a *flag* RST (RESET) ativa de modo a terminar a conexão instantaneamente. O número de total de pacotes transmitidos foi de 16 pacotes, num total de 2176 bytes.

Stream: 4 **Pacotes:** 217 - 226	3.186662 a 3.199381 **Duração:** 0.02749	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1141 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É criada uma conexão TCP onde não ocorreram erros no pedido HTTP GET "/moodle/lib/javascript-static.js". O servidor envia um código de resposta HTTP 304 *Not Modified* uma vez que o cliente já possui uma representação válida desse recurso (tal é provado e verificado através dos campos *If-None-Match* e ETag). Havendo um redirecionamento para o recurso presente em *cache*. O número de total de pacotes transmitidos foi de 10 pacotes, num total de 1409 bytes.
Stream: 5 **Pacotes:** 227 - 238	3.222860 a 3.531489 **Duração:** 0.308629	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1142 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	Estabelecida uma conexão TCP através do processo 3-way *Handshake* (pacote 227 a 229) sendo efetuado posteriormente, um pedido HTTP GET de "/moodle/lib/javascript-mod.php". Não se verificou a ocorrência de erros tendo sido transmitidos no total 989 bytes. O número de total de pacotes transmitidos foi de 9 pacotes, num total de 1503 bytes.
Stream: 6 **Pacotes:** 234 - 236; 239 - 245	3.516297 a 3.544831 **Duração:** 0.028534	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1143 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É iniciada uma conexão TCP onde não ocorreram erros no pedido HTTP GET "/moodle/lib/overlib.js". O servidor envia um código de resposta HTTP 304 *Not Modified* uma vez que o cliente já possui uma representação válida desse recurso (verificado através dos campos *If-None-Match* / ETag presentes nos cabeçalhos), sendo redirecionado para o recurso presente na *cache.* O número de total de pacotes transmitidos foi de 10 pacotes, num total de 1395 bytes.
Stream: 7 **Pacotes:** 246 - 255	3.582964 a 3.613962 **Duração:** 0.030998	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1144 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É estabelecida uma conexão TCP onde não ocorreram erros no pedido HTTP GET "/moodle/lib/cookies.js". O servidor envia um código de resposta HTTP 304 *Not Modified* uma vez que o cliente já possui uma representação válida desse recurso, sendo redirecionado para o recurso presente na *cache*. O número de total de pacotes transmitidos foi de 10 pacotes, num total de 1395 bytes.
Stream: 8 **Pacotes:** 256 - 265	3.617197 a 3.648826 **Duração:** 0.031629	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1145 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É estabelecida uma conexão TCP onde não ocorreram erros no pedido HTTP GET "/moodle/lib/ufo.js". O servidor envia um código de resposta HTTP 304 *Not Modified* uma vez que o cliente já possui uma representação válida desse recurso, sendo assim redirecionado para o recurso presente na *cache*. O número de total de pacotes transmitidos foi de 10 pacotes, num total de 1395 bytes.
Stream: 9 **Pacotes:** 266; 268 - 271; 274 - 276; 278; 280;	3.663604 a 3.713998 **Duração:** 0.050394	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1146 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É estabelecida uma conexão TCP e uma sessão HTTP onde não ocorreram erros no pedido HTTP GET "/moodle/lib/ufo.js". O servidor envia um código de resposta HTTP 304 *Not Modified* uma vez que o cliente já possui uma representação válida desse recurso, sendo assim redirecionado para o recurso presente na *cache*. O número total de pacotes transmitidos foi de 10 pacotes, num total de 1428 bytes.

***Stream*:** 10 **Pacotes:** 267; 272;273; 277; 279; 281;282; 284 - 285	3.675176 a 3.722428 **Duração:** 0.047252	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1147 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	Estabelecida uma conexão TCP através do processo 3-*way Handshake* sendo efetuado numa fase posterior, um pedido de uma imagem no formato GIF através de um HTTP GET de "/moodle/pix/spacer.gif". Após a receção do código da resposta HTTP 200 OK é terminada a sessão, não tendo sido encontrados erros na mesma. O número total de pacotes transmitidos foi de 10 pacotes, num total de 1555 bytes.
Stream: 11 **Pacotes:** 283; 288;289; 291; 293; 295 - 300; 302	3.716224 a 3.771711 **Duração:** 0.055487	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1148 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É estabelecida uma conexão TCP através do processo 3-*way Handshake* sendo efetuado numa fase posterior, um pedido HTTP GET de "/moodle/calendar/overlib.cfg.php". Após a receção do código da resposta HTTP 200 OK é terminada a sessão, não tendo sido encontrados erros nesta mesma. O número total de pacotes transmitidos foi de 12 pacotes, num total de 1726 bytes.
Stream: 12 **Pacotes:** 287; 290; 292; 294; 301; 303;304; 306 - 308	3.722807 a 3.779233 **Duração:** 0.056426	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1149 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	É estabelecida uma conexão TCP através do processo 3-way *Handshake* sendo efetuado numa fase posterior um pedido de uma imagem no formato JPEG através de um HTTP GET de "/moodle/theme/standardwhite/gradient.jpg". Após a receção do código da resposta HTTP 200 OK é terminada a sessão, não tendo sido encontrados erros nesta mesma. O número total de pacotes transmitidos foi de 10 pacotes, num total de 1939 bytes.
Stream: 13 **Pacotes:** 305; 310 - 313; 317 - 320; 322	3.775350 a 3.882527 **Duração:** 0.107177	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1150 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	Estabelecida uma conexão TCP através do processo 3-way *Handshake* sendo efetuado numa fase posterior, um pedido de uma imagem no formato GIF através de um HTTP GET de "/moodle/pix/t/switch_minus.gif". Após a receção do código da resposta HTTP 200 OK é terminada a sessão, não tendo sido encontrados erros nesta sessão. O número total de pacotes transmitidos foi de 10 pacotes, num total de 1667 bytes.
***Stream*:** 14 **Pacotes:** 309; 314 - 316; 321; 323;324; 236-238	3.782558 a 3.889159 **Duração:** 0.106601	**Src.;** endpub106.scom3.uminho.pt (106)-porta 1151 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	Estabelecida uma conexão TCP através do processo 3-way *Handshake* sendo efetuado numa fase posterior, um pedido de uma imagem no formato GIF através de um HTTP GET de "/moodle/pix/s/briggrin.gif". Após a receção do código da resposta HTTP 200 OK é terminada a sessão, não tendo sido encontrados erros nesta sessão. O número total de pacotes transmitidos foi de 10 pacotes, num total de 1746 bytes.
***Stream*:** 15 **Pacotes:** 325; 329-339	3.885260 a 3.903881 **Duração:** 0.018621	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1152 **Dest.:** endpub215.scom3.uminho.pt (215)-porta 80	Estabelecida uma conexão TCP através do processo 3-*way Handshake* sendo efetuado numa fase posterior, um pedido de uma imagem no formato GIF através de um HTTP GET de "/moodle/pix/moodlelogo.gif". Após a receção do código da resposta HTTP 200 OK é terminada a sessão, não tendo sido encontrados erros nesta sessão. O número total de pacotes transmitidos foi de 12 pacotes, num total de 4239 bytes.

***Stream*:** 16 **Pacotes:** 340 - 347; 425	17.040244 a 82.494246 **Duração:** 65.454002	**Src:** endpub106.scom3.uminho.pt (106)-porta 1153 **Dest:** rate-limited-proxy-66-249-91-17.google.com (66.249.91.17)-porta 80	Sessão HTTP entre o cliente e o servidor (mail.google.com), sendo possível observar o endereço de e-mail da conta com *login* (eu.nuno@gmail.com) e uma vez que a ligação foi feita através de HTTP (sem segurança adicional) poderá ver-se as mensagens trocadas (se tivesse sido usado HTTPS, não seria possível observar as mensagens trocadas), como mostra a Figura 1. A sessão de *login* é terminada no final da *stream*, recorrendo-se para isso a um pedido RST. O número total de pacotes transmitidos foi de 9 pacotes num total de 2842 bytes.
***Stream*:**17 **Pacotes:** 352 - 373	23.819398 a 35.186792 **Duração:** 11.367394	**Src:** endpub106.scom3.uminho.pt (106)-porta 1154 **Dest:** piano.dsi.uminho.pt (193.137.8.95)-porta 21	Sessão FTP entre o cliente (106) e o servidor (piano.dsi.uminho.pt), na qual foi possível observar uma tentativa de *login* no servidor FTP, utilizando o nome de utilizador "*anonymous*" (como mostra a Figura 2) que normalmente é utilizada por defeito nos servidores FTP públicos. Neste caso provou-se que o servidor já se encontra "protegido" por este tipo de possível ataque. O número total de pacotes transmitidos foi de 53 pacotes, num total de 3239 bytes.
Stream:18 **Pacotes:** 375 - 431	54.257406 a 82.845997 **Duração:** 28.588591	**Src.:** endpub106.scom3.uminho.pt(106)-porta 1156 **Dest.:** piano.dsi.uminho.pt (193.137.8.95)-porta 23	Sessão TELNET entre o servidor e o cliente (106), na qual foi possível observar uma tentativa de *login*, (possivelmente um ataque de *bruteforce*) com o uso de credenciais incorretas, como se observa na Figura 3. O número total de pacotes transmitidos foi de 14 pacotes, num total de 918 bytes.
Stream: 19 **Pacotes:** 435; 437; 442	97.001824 a 106.000754 **Duração:** 8.993732	**Src:** host222-58-static.28-87-b.business.telecomitalia.it (87.28.58.222)-porta 11132 **Dest:** endpub157.scom3.uminho.pt (157) -porta 30797	Tentativa por parte de um *host* com IP 87.28.58.222 de fazer vários pedidos "SYN", ao servidor endpub157.scom3.uminho.pt, na porta 30797, sendo que não obtém resposta por parte do servidor de destino e por isso continua a fazer pedidos de retransmissão (TCP *Retransmission)*. Possivelmente este *host* estaria a fazer um ataque DDOs ao servidor de destino. O número total de pacotes transmitidos foi de 3 pacotes, num total de 186 bytes.
***Stream*:** 20 **Pacotes:** 436; 439; 444	98.607890 a 107.601622 **Duração:** 8.993732	**Src:** host222-58-static.28-87-b.business.telecomitalia.it (87.28.58.222)-porta 11139 **Dest:** endpub157.scom3.uminho.pt(157) -porta 443	Tentativa por parte de um *host* com IP 87.28.58.222 de fazer vários pedidos "SYN", ao servidor endpub157.scom3.uminho.pt, na porta 443, sendo que não obtém resposta por parte do servidor de destino e por isso continua a fazer pedidos de retransmissão (TCP *Retransmission*). Possivelmente este *host* estaria a fazer um ataque DDOs ao servidor de destino. O número total de pacotes transmitidos foi de 3 pacotes, num total de 186 bytes.
***Stream*:** 21 **Pacotes:** 438; 440; 446	100.221796 a 109.203745 **Duração:** 8.981949	**Src:** host222-58-static.28-87-b.business.telecomitalia.it (87.28.58.222)- porta 11141 **Dest:** endpub157.scom3.uminho.pt (157) -porta 80	Tentativa por parte de um host com IP 87.28.58.222 de fazer vários pedidos "SYN", ao servidor endpub157.scom3.uminho.pt, na porta 80, sendo que não obtém resposta por parte do servidor de destino e por isso continua a fazer pedidos de retransmissão (TCP *Retransmission)*. Possivelmente este *host* estaria a fazer um ataque DDOs ao servidor de destino. O número total de pacotes transmitidos foi de 3 pacotes, num total de 186 bytes.

Stream: 22 **Pacotes:** 451 - 458	137.534994 a 137.997816 **Duração:** 0.462822	**Src:** endpub106.scom3.uminho.pt (106)-porta 1157 **Dest:** rate-limited-proxy-66-249-91-1 7.google.com (66.249.91.17)-porta 80	Sessão HTTP entre o cliente e o servidor (mail.google.com), sendo possível observar o endereço de e-mail da conta com *login* (eu.nuno@gmail.com) e uma vez que a ligação foi feita através de HTTP (sem segurança adicional) poderá ver-se as mensagens trocadas (se tivesse sido usado HTTPS, não seria possível observar as mesmas). Comparativamente ao que aconteceu na *stream* 16, nesta *stream* não é terminada sessão, podendo haver o risco de *Session hijacking*, sobretudo devido ao facto de existirem *cookies* do site (ver Figura 4), que podem pôr em risco os dados associados ao *login* do referido e-mail. O número total de pacotes transmitidos foi de 8 pacotes, num total de 2788 bytes.
Stream: 23 **Pacotes:** 461 - 563	143.664551 a 152.818884 **Duração:** 9.1473374	**Src:** endpub106.scom3.uminho.pt (106)-porta 1158 **Dest:** endpub142.scom3.uminho.pt (142)-porta 445	Sessão SMB entre o cliente (106) e o servidor endpub142.scom3.uminho.pt. Este protocolo é normalmente usado por sistemas operativos Windows (ver Figura 5), para partilha de ficheiros, sendo o mesmo vulnerável (devido às fracas medidas de segurança) a vários tipos de ataques. Pode-se observar no pacote 472, que existe uma tentativa de login com o *user "root"* ("\"), (Ver Figura 6) ao diretório \\TROMBONE\IPC (ver Figura 7), mas a mesma foi recusada, como comprova o pacote 475 (ver Figura 8). Houve também uma tentativa de *login* com o *user* "BOCASJNR\hsantos" (ver Figura 9), ao diretório \\TROMBONE\SOFT (ver Figura 10), tendo este tentado aceder ao ficheiro "\AutoRun.inf" (ver Figura 11) (como prova o pacote 484), mas sem sucesso, como mostra a Figura 12. Nesta sessão houve também pacotes que foram perdidos e foram de seguida retransmitidos através TCP *Retransmition* O número total de pacotes transmitidos foi de 98 pacotes, num total de 17 Kbytes.
Stream: 24 **Pacotes:** 464; 467;469	143.676901 a 143.720977 **Duração:** 0.044076	**Src:** endpub106.scom3.uminho.pt (106)-porta 1159 **Dest:** endpub142.scom3.uminho.pt (142)-porta 139	Tentativa de estabelecimento de ligação com o servidor endpub142.scom3.uminho.pt como prova o pacote 464 (ver na Figura 13), mas sem sucesso, tendo a mesma sido terminada com um pacote RST (ver Figura 14). O número total de pacotes transmitidos foi de 3 pacotes, num total de 178 bytes.

UDP

Nº ordem ou *streams*	Tempo (s)	Src/Dest	Comentário
Stream: 0 **Pacotes:** 348; 350	23.779650 a 23.792078 **Duração:** 0.012428	**Src.:** endpub106.scom3.uminho.pt (106)-porta 1030 **Dest.:**endpub142.scom3.uminho.pt (142)-porta 53	Pedido DNS feito pelo *hos*t (106) ao servidor endpub142.scom3.uminho.pt para este lhe responder qual o ip do dns “piano.dsi.uminho.pt”, ao que este responde “193.137.8.95”.
***Stream*: 7** **Pacotes:** 462	**Duração:** 0	**Src.:**endpub142.scom3.uminho.pt (142)-porta 137 **Dest.:** endpub106.scom3.uminho.pt (106)-porta 137	Pedido NBNS (NetBIOS Name Service) que serve para traduzir o dns do serviço NETBIOS presente na *stream* TCP nº23, para um endereço IP.

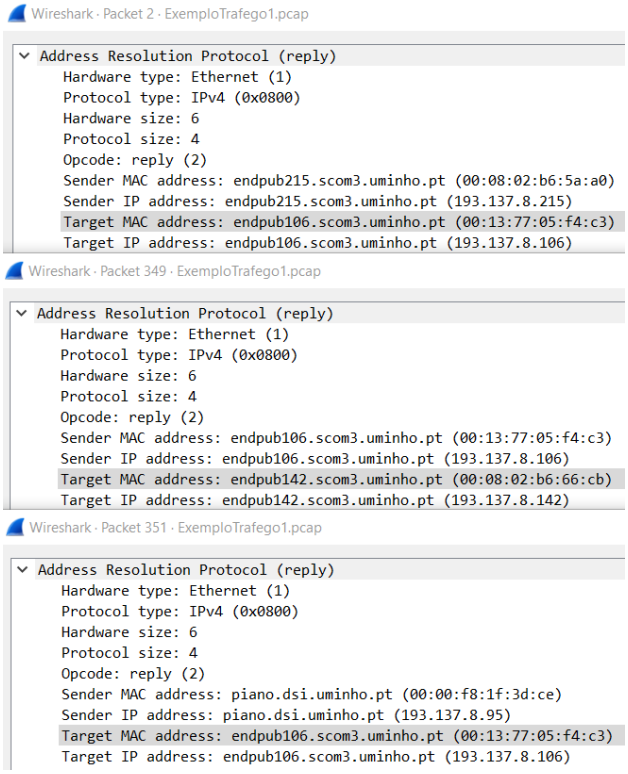
No que diz respeito às *streams* de 1 a 6, as mesmas não apresentam dados suscetíveis de poderem ser estudados, bem como o conteúdo dos seus pacotes não mostra informações possíveis de serem decifradas.

ICMP

Nº ordem	Tempo (s)	Src/Dest	Comentário
Pacotes: 1; 362; 396 432; 448; 540	23.779650 a 23.792078 **Duração:** 0.012428	**Src:** 193.137.88.13 (endpub013.scom-glt.uminho.pt) **Dest:** 172.16.170.81	De modo a testar a conectividade foram efetuados sucessivos “Ping Request”, espaçados de 30 segundos, sem qualquer resposta “Ping Reply”.
Pacotes: 441	**Duração:** 0	**Src:** 172.16.40.125 **Dest:** 172.16.170.81	Realizado “Ping Request” sem qualquer resposta “Ping Reply”.
459;460	143.654404 a 143.660955 **Duração:** 0.006551	**Src:** (106) endpub106.scom3.uminho.pt **Dest:** (142) endpub142.scom3.uminho.pt	O (106) efetuou um “Ping request” para o (142) tendo recebido do mesmo uma resposta “Ping Reply”, desta forma esta conexão é valida e pode ser utilizada.

ARP

O protocolo ARP é utilizado para descobrir o endereço físico (MAC) de um host através do endereço IP do mesmo. Deste modo, no pacote 2, 349 e 351 encontra-se representado a descoberta dos endereços MAC's de (106) e (142).



Informações sobre os endereços de IP externos à *home net*

87.28.58.222→ Telecom Italia S.p.A.(Roma, Itállia)

41.244.211.188→ VIETTEL-CMv4-I (Yaounde, Camarões)

66.249.91.17 – GOOGLE (Mountain View, Estados Unidos)

81.64.154.175 - FR-NCNUMERICABLE (França)

84.41.174.73 - NL-QINIP-20040908 (Holanda)

84.91.17.250 – NOWO (Portugal)

172.16.40.125 - PRIVATE-ADDRESS-BBLK-RFC1918-IANA-RESERVED (Los Angeles, Estados Unidos)

172.16.170.81 - PRIVATE-ADDRESS-BBLK-RFC1918-IANA-RESERVED (Los Angeles, Estados Unidos)

Informações adicionais de estatística

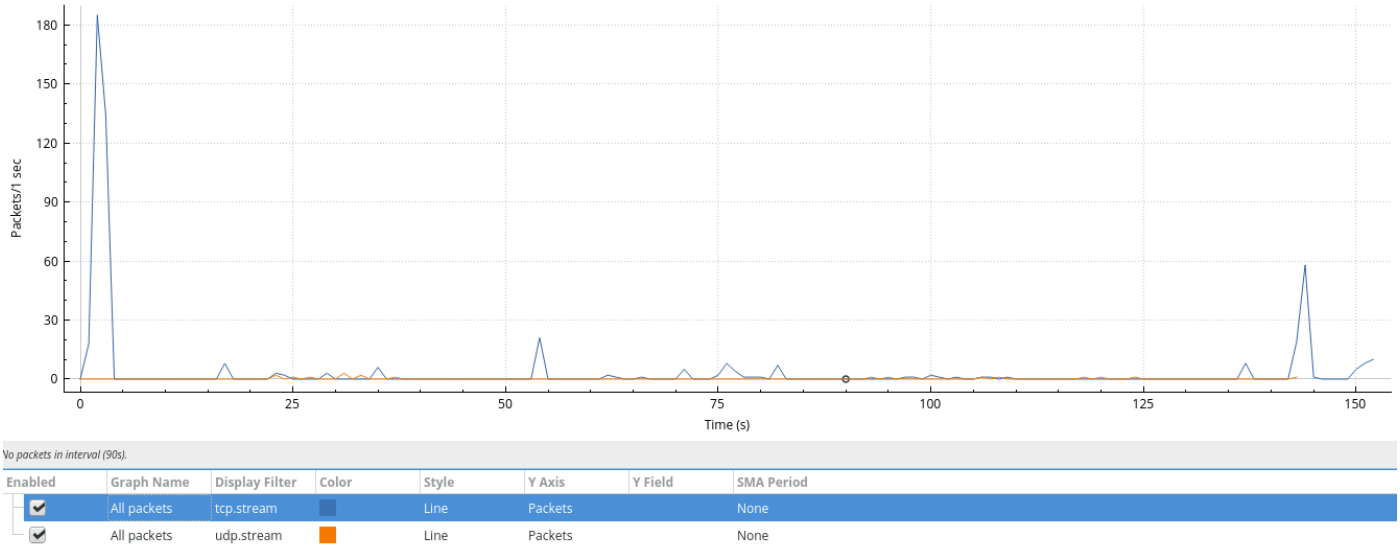
Através do Wireshark foi possível observar as propriedades do ficheiro de captura, tais como:

Data da captura: 2007-10-16
Duração da captura: 00:02:32
Pacotes capturados: 563
Total de bytes capturados: 185889

Iniciando uma análise estatística com uma abordagem geral, verifica-se que o protocolo predominante é o TCP com uma percentagem de 95.16 %, de seguida encontra-se em 3.23 % dos pacotes o UDP e por fim 1.61% do tráfego são outros tipos de protocolos.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
IP Protocol Types	558				0,0037	100%	1,5000	2,206
UDP	18				0,0001	3,23%	0,0200	23,780
TCP	531				0,0035	95,16%	1,5000	2,206
NONE	9				0,0001	1,61%	0,0200	143,654

Recorrendo à ferramenta do Wireshark (I/O Graph), e usando devidamente os filtros “tcp.stream” e “udp.stream”, obtemos o seguinte gráfico, no qual é possível observar que existe um maior fluxo de dados TCP em detrimento do UDP, havendo um grande número de pacotes no início da captura e no final da mesma.



Anexo de Figuras

```
GET /mail/?ui=pb&tlt=115a67ba1f3 HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; GNotify 1.0.25.0)
Host: mail.google.com
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: GV=10115a9980eb7-6dec08d9f1dfd9f8b6151b4afca9a9f4;
__utma=173272373.870200234.1175466843.1175466843.1175466843.1; gmailchat=eu.nuno@gmail.com/104902; S=gmail=2BOv8-
GZ5SSMzZQu8Lkpwg:gmail_yj=7gECZkY1yCB029onOc6XoQ:gmproxy=jd3pMfLR7ic:gmproxy_yj=kKwdq9Ty1Gc:gmproxy_yj_sub=W8G-7fLAEk0;
PREF=ID=77a64c6088f3ea1c:TM=1167250258:LM=1167250258:S=USGBHPfj9i5dGP-M;
SID=DQAAAHkAAAAzEF93tOOV4RhNJywuq0A1qO5Kl5D7fy7oHDx6tbyp6nrUjce49LXvmTkdYgVSBhdtsnX0poppXnB9nv56CSWQ9q2mEV_nXu0ibW2phTgj
3Rc6YXkRAlyGjUl1F-ByEOqDnPr0zp16S8nAnj6oJLkIL-9XdD0ZpU7Fc2VkDtbnWQ

HTTP/1.1 200 OK
Cache-control: no-cache, no-store
Pragma: no-cache
Content-Type: application/octet-stream
Content-Length: 1422
Server: GFE/1.3
Date: Tue, 16 Oct 2007 16:36:34 GMT


.................."...^all...^i...^u..7
1
.membership@techtarget.com.au..SearchStorage ANZ.........ETape encryption; Exchange Backup; 4PB of tape; Google's
storage plans..0SearchStorage ANZ : Weekly Site RoundUp &hellip;...
.................."...^all...^i...^u..(
"
.program@mentornet.net.          MentorNet..........[MentorNet DS]: Interviews..eFor Match with Sam Bartels) Henrique,
Giving a good interview is a skill that we often learn &hellip;...
.................."...^all...^i...^u..4
.
.membership@techtarget.com.au..TechTarget ANZ.........HNew White Papers: Intelligent storage; Security risk reduction;
and more..jTechTarget ANZ : White Paper Update Welcome to TechTarget ANZ&#39;s White Paper Update, featuring &hellip;...
.................."...^all...^i...^u..8
2
```

Figura 1

```
220 piano.dsi.uminho.pt FTP server (Digital UNIX Version 5.60) ready.
USER anonymous
530 User anonymous unknown.
QUIT
221 Goodbye.
```

Figura 2

```
.
.
Digital UNIX (piano.dsi.uminho.pt) (ttyp1)
.

.
.

....login: guest
guest
Password:guest

Login incorrect


Wait for login retry ...

Login incorrect
login: .^D..
```

Figura 3

```
Cookie: GV=10115a9980eb7-6dec08d9f1dfd9f8b6151b4afca9a9f4;
__utma=173272373.870200234.1175466843.1175466843.1175466843.1; gmailchat=eu.nuno@gmail.com/104902; S=gmail=2BOv8-
GZ5SSMzZQu8Lkpwg:gmail_yj=7gECZkY1yCB029onOc6XoQ:gmproxy=jd3pMfLR7ic:gmproxy_yj=kKwdq9Ty1Gc:gmproxy_yj_sub=W8G-7fLAEk0;
PREF=ID=77a64c6088f3ea1c:TM=1167250258:LM=1167250258:S=USGBHPfj9i5dGP-M;
SID=DQAAAHkAAAAzEF93tOOV4RhNJywuq0A1qO5Kl5D7fy7oHDx6tbyp6nrUjce49LXvmTkdYgVSBhdtsnX0poppXnB9nv56CSWQ9q2mEV_nXu0ibW2phTgj
3Rc6YXkRAlyGjUl1F-ByEOqDnPr0zp16S8nAnj6oJLkIL-9XdD0ZpU7Fc2VkDtbnWQ
```

Figura 4

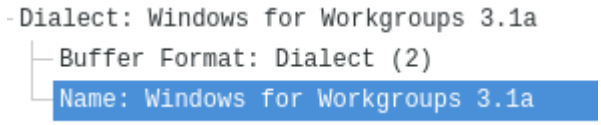


Figura 5

```
Session Setup AndX Request, NTLMSSP_AUTH, User: \
```

Figura 6

```
Tree Connect AndX Request, Path: \\TROMBONE\IPC$
```

Figura 7

```
Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
```

Figura 8

```
Session Setup AndX Request, NTLMSSP_AUTH, User: BOCASJNR\hsantos
```

Figura 9

```
Tree Connect AndX Request, Path: \\TROMBONE\SOFT
```

Figura 10

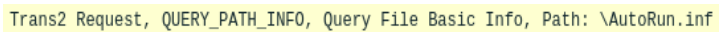


Figura 11

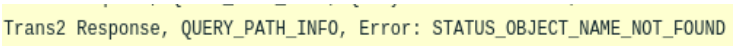


Figura 12

Figura 13

Figura 14